



Revista de Networking y Programación
www.nexweb.com.ar
NEX # 10 - Agosto 2004 - Precio Argentina 4 $
(Recargo interior del país 0,20 $)
/ Bolivia 10 $ / Chile 1500 $ / Mexico 15 $ / Paraguay 9000 Gs / Uruguay 35 $ / Peru 5,5 ns / Venezuela 2000 bs

ISSN 1668-5423
9 771668 542003 00010

Patrocinadores Diamante







21 al 24 de Septiembre

La Rural, Buenos Aires

EXPO COMM / IT ARGENTINA 2004 se transformó ... Por eso hoy se presenta como un evento único en su tipo en todo América Latina, con + de 150 **Empresas Expositoras** y nuevos **Atractivos Especiales.**

- **SEMINARIO DE TECNOLOGIA Y MERCADO** Un nuevo y renovado Ciclo Académico será el eje de la capacitación y el conocimiento en esta nueva edición.
- **CONVERGENCE CENTER** Conozca las soluciones de redes empresariales que pueden cambiar el ritmo de los negocios de su empresa.
- **CONTACT CENTER EN VIVO** Sepa por qué el e-CRM y el Contact Center son factores imprescindibles en las nuevas estrategias de negocios orientados al cliente.



>> 100% tecnología y negocios

Regístrese HOY mismo a la Exposición y Seminario en

http://www.expocomm.com.ar/cortech

Organizan







Auspicios Oficiales





PB040720-B

Los menores de 18 años, estando incluso estos, acompañados por un mayor NO PODRAN INGRESAR a la exposición bajo ningún motivo y circunstancia



Editorial

Bienvenido a *NEX IT Specialist.*

La revista que tienen en sus manos es la continuación de "NEX, periódico de Networking y Programación". Y seguimos creciendo. Evolucionamos del formato periódico a revista de forma natural por vuestra demanda, soporte y aceptación. Tal como hicimos hace casi dos años en nuestra primera edición (NEX 1) deseamos antes que nada, decirles a quién está dirigido y cuál es el nivel de sus artículos.

NEX IT Specialist, está dirigido a aquellos con interés y que están activos en IT (Information Technology): en redes y programación. También será de mucha utilidad para quienes se encuentren capacitando en IT y para estudiantes universitarios de las carreras de sistemas y/o quienes estén realizando las certificaciones internacionales de CISCO, Microsoft (MCSE, MCSA, MCSD, MCDBA), Linux (LPI, Linux+, RHCE) y otras.

IT evoluciona tan rápidamente que se hace casi imposible mantenerse al día en las últimas tecnologías. Alguno puede responder: pero en Internet puedo encontrar todo. Si está todo: buenos artículos, malos artículos, buenas traducciones, malísimas traducciones. Lleva mucho tiempo distinguir lo bueno de lo malo. En ***NEX IT Specialist*** daremos un claro y resumido informe sobre una dada temática muy actual y bibliografía seleccionada.

Habrá artículos que servirán de introducción. Otros serán más especializados. Además, tendremos artículos estructurados como una serie y que llamaremos Paso a Paso. Siempre, todos caracterizados por la claridad y el mejor nivel.

En este ejemplar inauguramos tres Paso a Paso: "Fundamentos de seguridad Informática", "Ethical Hacking" y "Clusters".

NEX IT Specialist llenará un espacio no cubierto por otras publicaciones del mercado, orientando al lector a temas específicos, bibliografía, cursos y carreras del mundo IT.

Muchas veces usaremos términos en inglés (con su correspondiente traducción) ya que creemos que toda persona con altas miras en esta actividad deberá de a poco lograr un dominio de ese idioma. De este modo podrá aprovechar toda la bibliografía disponible.

Buscaremos un balance entre los diferentes sistemas operativos que hoy rigen el mercado Linux y Windows. Dada su importancia y vigencia haremos un especial énfasis en desarrollar temas de seguridad informática.

Si UD. está en IT, considere a ***NEX IT Specialist*** como su revista. Intentamos representar a la comunidad IT. Para ello hemos convocado a un grupo de expertos que aportan sus conocimientos mes a mes, junto al humor de Marcos Severi.

Esperamos contar con Ustedes para tener un feedback a nuestra oferta. No duden en contactarnos y aquellos que quieran recibir la revista lo podrán hacer suscribiéndose a través de nuestro web site.

Para finalizar les comento que hemos inaugurado un nuevo newsletter mensual: *Reports en IT* por Carlos Vaughn-O´Connor. Estos son reportes muy resumidos de temas que no se pueden desconocer. Ya salió Report IT #1. Aquellos que los deseen recibir gratuitamente podrán suscribirse en www.cortech.com.ar.

I.T. NEX SPECIALIST

Revista de Networking y Programación

Año 3 - Número 10 - Agosto 2004

Staff

Director
Dr. Osvaldo Rodríguez

Propietarios
COR Technologies S.R.L.

Coordinador Editorial
Carlos Rodríguez Bontempi

Responsable de Contenidos
Dr. Osvaldo Rodríguez

Editores
Raúl Kuzner
Juan Manuel Zolezzi

Correctores
María Lujan Zito

Redactores
Javier Pierini,
Juan Manuel Zolezzi,
Osvaldo Rodríguez,
María Luján Zito,
Leonel F. Becchio,
Rodrigo M. González,
Hugo Cela,
Guido Lorenzutti.
Dr. Reinaldo Pis Diez.

Humor
Marcos Severi

Distribución
Ximena Antona,
Victor Pereyra

Diseño Web Site
Emanuel A. Rincón

Diseño Gráfico
Víctor Pereyra
Carlos Rodríguez Bontempi

Publicidad
Ximena Antona
publicidad@nexweb.com.ar

Preimpresión e Impresión
Impresión: IPESA Magallanes 1315. Capital Federal. Tel 4303-2305/10

Distrbución
Distribución en Capital Federal y Gran Buenos Aires: HUESCA-SANABRIA. Baigorri 103. Capital Federal. Tel 4304-3510
Distribuidora en Interior: Distribuidora Austral de Publicaciones S.A. Isabel la Católica 1371.
Capital Federal. Tel. 4301-0701

NEX - Periódico de Networking
Registro de la propiedad Intelectual en trámite [illegible]

ISSN 16685423

Dirección: Av. Córdoba 657, Piso 12
C1054AAF - Capital Federal
Tel: +54 (11) 4312-7694
http://www.nexweb.com.ar

El staff de NEX colabora ad-honorem, si desea escribir para nosotros, enviar un e-mail a: articulos@nexweb.com.ar








Indice

Sumarios Paso a Paso:

FUNDAMENTOS DE SEGURIDAD INFORMATICA, PASO A PASO
FUNDAMENTOS DE ETHICAL HACKING, PASO A PASO

La herramienta más importante que tienen los administradores de red para proteger sus redes es el "conocimiento".
En este y futuros números de *NEX IT Specialist* iremos desarrollando una serie de artículos donde en forma clara y resumida expondremos los temas más fundamentales en los que se basa la seguridad informática. Hemos dividido la presentación en dos partes: por un lado los fundamentos. Por el otro las herramientas.
En los fundamentos veremos entre otros temas como: Elementos Básicos de criptografía (I y II), Entendiendo TCP/IP, Autenticación Kerberos, Public Key Infrastucture (PKI) (incluirá temas como Cerificados y Pretty Good Privacy (PGP)). Comunicaciones seguras (SSL, SSH, IPsec, VPNs). Protocolos de tuneleo (PPTP, L2TP).
En las herramientas: ¿Que es Ethical Hacking?, Footprinting.

CLUSTERS PASO A PASO

En una serie de artículos entenderemos los diferentes tipos de clusters, la diferencia entre openMosix y Condor con Beowulf.
También veremos que ofrece Microsoft bajo su arquitectura en maquinas en clusters. Finalmente ahondaremos en "Grid Computing".




WEBLOGS



Desde los comienzos de la implementación de esta nueva tendencia en comunicaciones a mediados de la década pasada hasta ahora, los WEBLOGS o BLOGS han mostrado un marcado aumento de popularidad que los han posicionado en lugares tan diversos como problemáticos ofreciendo la posibilidad de examinar una gran cantidad de fuentes de información publicada en cientos de sitios en un solo lugar.

Fundamentos

Si uno publica en un sitio un periódico o revista y el contenido cambia con regularidad, el uso de un CMS (Content Management Systems) brindará mucha ayuda en lo que respecta a la administración de la información. Después de todo, ¿por qué modificar manualmente enaces, títulos u otros detalles si existe una aplicación que realiza estas tareas por nosotros?.

Tradicionalmente, las aplicaciones de administración de contenido (CMS Content Management Systems) para sitios WEB son grandes y complejas ya que deben preveer todo tipo de contingencias de muchas organizaciones en las que pueden estar instaladas. En determinados casos podría permitirse que algunas personas estén al frente de la tarea de generar documentación para publicar y en otros no, también pueden variar los estilos o el método de búsqueda o muchas otras cosas más.

Este tipo de aplicaciones de administración de contenidos puede resultar complejo de instalar y mantener en algunas estructuras que manejan publicaciones sencillas pero que presentan cambios a intervalos regulares. Como respuesta a la complejidad de las aplicaciones CMS encontramos una alternativa en las aplicaciones de manejo de WEBLOGS.

Los WEBLOGS comenzaron a aparecer en los 90´s como periódicos personales. Diarios personales que permiten a un individuo escribir y publicar artículos fácil y rápidamente y aunque los BLOGS varían mucho en estilo sus formatos son bastante uniformes, lo que reduce la complejidad de la aplicación que lo maneja haciendo muy simple su implementación y administración.

Si nunca vio un BLOG, puede ingresar a la dirección http://www.weblogs.com.ar/ para tener una idea de lo que representan, significan y puede hacerse con ellos.

¿Cómo se compone un WEBLOG?

Los WEBLOGS pueden tener diversas presentaciones de formas y medidas lo que permite reflejar los intereses y estilo del autor, pero citaremos las características comunes para tener una idea aproximada de sus propiedades:

Orden

Las publicaciones se muestran en orden inverso presentando siempre el más reciente al tope de una corta lista de artículos, permitiendo el acceso al resto de las publicaciones como una extensión de la aplicación.

Comentarios

Los lectores de un WEBLOG pueden contribuir con comentarios a los artículos publicados. En este sentido un WEBLOG se parece bastante a un foro excepto que aquí no se puede iniciar una discusión no presentada en un artículo.

Autoría

Típicamente solo una persona se adjudica la autoría de un WEBLOG aunque existen algunos escritos con varios colaboradores. Los comentarios son escritos por otra gente que no está dentro de esta categoría.

Disponibilidad (Syndication)

El contenido de un WEBLOG generalmente se hace utilizando un formato XML conocido como RSS (Really Simple Syndication). Esto hace posible la recuperación, análisis y recolección de información de diversas fuentes dando lugar a una suerte de periódico personalizado.

Seguimiento (Trackback)

Término acuñado por la aplicación propietaria Movable Type que nos da la posibilidad de hacer el seguimiento de los enlaces entre los sitios en que se aloja la información.

Edición basada en WEB

Algo primordial ya que los WEBLOGS existen sólo en la WEB y se supone que cada entrada al BLOG sea iniciada desde un navegador. Aunque sea molesto pensar en un navegador para escribir un artículo existen aplicaciones de escritorio que permiten trabajar con un documento en un formato de edición de texto y luego subir el trabajo terminado de manera más eficiente. Un buen ejemplo de esto es el proyecto Epoz.

Funcionabilidad

Desde sus comienzos como medio para brindar información de manera actualizada en un formato eficiente hasta la proliferación de numerosos sitios que lo utilizan para mantener un contacto informativo más estrecho con sus visitantes, los BLOGS han pasado por una serie de etapas y cambios que lo han convertido en el medio de información de crecimiento sostenido más rápido de los últimos tiempos.

El hecho es que tanto grupos de estudiantes que quieren dar a conocer sus opiniones como candidatos presidenciales lo utilizan como medio para comunicar opiniones y pareceres a quien quiera leerlos.

Por ejemplo, en las últimas elecciones del partido demócrata norteamericano, cada candidato tenía al menos un servicio de información basado en BLOGS que sus asesores políticos controlaban y configuraban para analizar estadísticamente la opinión de los ciudadanos interesados.

Aplicaciones I: Blosxom

Dentro del abanico de aplicaciones preparadas para manejar este tipo de información podemos destacar BLOSXOM, una aplicación escrita en PERL y diseñada para ser ejecutada como una aplicación CGI en un servidor web escrita por Rael Dornfest, un programador de O'Reilly & Associates.

Si es de los que presuponen que una aplicación que consume pocos recursos no puede realizar demasiadas tareas está equivocado. Adicionalmente a su capacidad de manejo de información debemos sumarle la flexibilidad para el usuario de mezclar y combinar funcionalidades.

Instalación

Si tiene cierto manejo fluído de un servidor WEB, entonces la instalación de la aplicación será sencilla. Consiste de un único programa escrito en PERL que tendrá que copiar a su directorio de CGI.

Listo. Ya puede ejecutarlo.

Por supuesto que sabemos que cada aplicación requiere una configuración, mínima si se quiere, pero debemos dedicarle cierto tiempo si queremos que funcione según nuestras expectativas.

En el comienzo del programa podremos encontrar una serie de variables que utilizaremos para configurarlo según nuestro gusto y gracias a la abundante documentación de este archivo, la funcionalidad de cada una de estas variables se vuelve una tarea sencilla de comprender y, según necesitemos, modificar.

Por ejemplo, podemos comenzar con la configuración de ciertos parámetros básicos:

$blog_title: el título que aparecerá en los mensajes y en los RSS.

$blog_description: descripción del BLOG en la página principal del RSS.

$datadir: cada entrada del BLOG es un archivo de texto ubicado en el directorio definido aquí.

Ahora está funcionando con un cierto toque personal.

Agregando entradas

Por ejemplo, si creamos el archivo de presentación $datadir, ejemplo.txt:

Entrada de ejemplo.

<p>¡Hola!</p>

Si bien parece un ejemplo sencillo, (de hecho lo es), es interesante ver como se puede cambiar el aspecto al mostrarse en el BLOG, precedido por la fecha, seguido por la hora y un enlace, con la primera línea en negrita como un título.

En otras palabras, se pueden agregar entradas simplemente creando archivos de texto plano en el directorio definido anteriormente. Cualquier archivo con extensión .TXT será tomado en cuenta como una entrada para el BLOG pero, por ejemplo, los archivos de copia de seguridad de Emacs, que agregan un ~ al final del nombre del archivo, no serán consideradas entradas para el BLOG. Ahora bien, si es de los que a medida que escriben, graban el archivo frecuentemente, se encontrará con una característica adicional: el archivo que está escribiendo estará disponible inmediatamente al público.

Si quiere verificar el aspecto de su BLOG, basta ingresar a la dirección:

http://localhost/cgi-bin/blosxom.cgi

La hora de creación del archivo será la que se agregue como información de cada entrada, pero por cuestiones administrativas podríamos querer cambiar este valor. Por ejemplo, si creamos un archivo el 20 de mayo de 2004 a las 13:15, dicha entrada se vería así:

ejemplo.txt 200405201315

Y ejecutando el comando:

touch -t 200405251234 ejemplo.txt

Aparecerá la entrada modificada con la fecha 25 de mayo de 2004 a las 12:34. Si el archivo propuesto no existe, se creará con ese criterio. Este paso, si bien va en contra de la filosofía propia de los BLOGS, puede realizarse por cuestiones de ajustes o para mejorar la administración o navegabilidad del sitio. De hecho, podría cambiar la fecha de un archivo a futuro.

Por ejemplo, si definimos la variable $show_future_entries con el valor 1, las entradas con esas características se verán siempre, pero usando la configuración predeterminada las entradas se verán únicamente cuando su fecha se corresponda con la fecha actual. Una característica útil, por ejemplo, para programar la publicación de ciertas entradas.

Si esta revisión terminase aquí seguramente no estaría muy convencido de las posibilidades de este programa, pero luego de examinar un poco más a fondo las opciones, se puede determinar que tiene un buen potencial. Este potencial se basa en la utilización de plantillas y en las características de los agregados que pueden utilizarse. Una de ellas, la predeterminada, utiliza el formato HTML y la segunda, opcional, RSS.

La manera de intercambiar esta plantilla es tan sencilla como definirla en la dirección de acceso a la información:

http://localhost/cgi-bin/blosxom.cgi para el formato HTML

http://localhost/cgi-bin/blosxom.cgi?flav=rss para el formato RSS.

Además, puede ahorrarse este trabajo configurando directamente su página como índice apropiado como en el ejemplo

http://localhost/cgi-bin/blosxom.cgi/index.rss

Del mismo modo que creamos un archivo de texto crearemos ahora uno en formato HTML o con la extensión RSS según sea el tipo de información que queramos mostrar.

Si bien existe una buena cantidad de información en el sitio oficial, podemos modificar ligeramente un archivo para acceder a las variables más comunes. Por ejemplo, los archivos reciben la información contenida en las variables $title y $body, entre otras, pero podría querer cierta configuración específica en mi sitio, por ejemplo, un texto alineado y con un título sobresaliente:

```
<p>
<H1 align="right">$title</h1>
<br />
$body
</p>
```

Este ejemplo inserta el contenido completo de la variable $body en el cuerpo de la página, evitándonos la tarea de conocer programación HTML, pero si quisiésemos, por ejemplo, agregar líneas en blanco en nuestra información, debemos usar algún programa para asistirnos. Afortunadamente Blosxom lo simplifica utilizando agregados

Agregados

Cada agregado en un programa escrito en PERL con las funciones necesarias para leer y evaluar una porción de código en particular. Cada archivo contenido en el directorio de agregados, definido por la variable $plugin_dir, es un agregado que se carga y ejecuta en orden alfabético.

La clase de características que puede encontrar utilizando estos agregados está limitada por unas pocas restricciones, pero mayormente podemos hacer lo que necesitemos con algún que otro agregado: cambiar la manera en que se recuperan los archivos de información, el modo en que se muestran las entradas del BLOG, las plantillas utilizadas para mostrar las entradas o el contenido de las mismas.

Si bien en el sitio oficial existe una buena cantidad de agregados, debe tenerse en cuenta que algunos requieren ciertas condiciones para su utilización. Por ejemplo el calendario, que necesita una versión que lo soporte para poder mostrarse correctamente..

Escribiendo agregados

El listado 1 contiene un filtro simple que hace que el nombre de la empresa aparezca en negrita cada vez que figure en una entrada.

Listing 1. negrita.pl

```
#!/usr/bin/perl
use strict;
use warnings;
use diagnostics;
package egotrip;
        # devuelve el valor 1 para
    indicar que está activo
sub start
{
 return 1;
}
        # pone el nombre en negrita
        sub story {
    my ($pkg, $path, $filename,
$story_ref,
      $title_ref, $body_ref) = @_;
     $$body_ref =~
```



```
s|CORTECH|<b>CORTECH</b>|g;
 1;
}
    1;
```

Pero podríamos hacerlo un poco más sofisticado insertando enlaces automáticos a una serie de elementos:

```
$$body_ref =~ s|(CORTECH)|
<a href="http://www.cortech.
com.ar/">$1</a>|g;
```

Con lo que cada porción de texto ubicada entre corchetes pasará a ser un enlace automático a la dirección especificada.

Aplicaciones II: El Reto a Enfrentar

Al momento de elegir una aplicación de administración de BLOGS nos enfrentamos a una tarea ardua que demanda cierto tiempo: ¿qué debemos hacer prevalecer al momento de elegir?, bueno, inicialmente debemos fijarnos una serie de premisas como las que comentamos anteriormente para poder elegir de manera apropiada.

Por ejemplo, si buscamos algo de rápida configuración, o de mantenimiento sencillo, o con amplias capacidades de búsqueda u otras características que nos interesen particularmente. Podemos hacer una extensa lista pero nos centraremos en las aplicaciones más conocidas:

ONGOING

En este sitio puede verse el desarrollo del programador Tim Bray, tan interesado en BLOGS que al no encontrar ninguna aplicación que le satisfaciese, decidió programar por su cuenta hasta conseguir lo que quería. Si bien puede resultarle parecido a la reinvención de la rueda, muchas veces nuestras espectativas nos llevan a esto cuando nos encontramos con la posibilidad de mejorar las prestaciones de una aplicación de administración de BLOGS, pero sin duda no es necesario llegar a este punto.

Para más información puede visitar el sitio en la dirección http://www.tbray.org/ongoing.

CoreBLOG

Un muy buen administrador de BLOGS pero que depende de una aplicación para servidores llamada Zope orientada a la administración de bases de datos (ZODB) y ciertamente compleja de configurar y administrar.

Manila

Ofrece una alternativa con un importante costo de implementación pero también puede obtener una copia de prueba que incluye un plazo de gracia para implementar su servidor de RSS en su sitio.

Opinión 1: Blosxom

BLOSXOM es una herramienta poderosa para la administración y creación de BLOGs, mucho mejor de lo que puede llevarnos a creer nuestra primera impresión.

Se instala de manera sencilla y la tarea de configuración se hace prácticamente sola siguiendo la documentación del mismo único archivo. Además permite la configuración de la plantilla de salida y de cada elemento de la misma ya sea utilizando variables o agregados específicos.

Opinión 2: El reto a enfrentar

La administración de contenidos en un sitio orientado al manejo de información en forma de BLOGS dependerá exclusivamente del tipo de trato que queramos darle a la información expuesta y la facilidad con que estemos interesados en disponer de ella.

Más allá de las opciones vistas en este artículo tendremos posibilidad de probar antes de efectivizar una sección de este tipo en nuestro sitio.

Conclusión

Así como la línea editorial de los periódicos ha cambiado para adaptarse a los tiempos que corren, también los sitios WEB deben adaptarse a las nuevas tecnologías con el propósito de brindar la mejor información de la mejor manera posible, con la mayor confiabilidad y la rapidez de estos tiempos.

Para llenar este nuevo espacio parecen haber aparecido, o mejor dicho reaparecido, repentinamente como novedad, los BLOGS.

Estará en los administradores de sitios WEB y en los profesionales dedicados al manejo de información poner sus recursos a disposición de los visitantes utilizando este tipo de implementaciones.

Hugo R. Cela
ITC

Direccionario

La comunidad de weblogs argentinos
http://www.weblogs.com.ar
Blosxom: sitio oficial
http://www.blosxom.com
Blox: formateo de texto
http://www.enilnomi.net/download.html#blox
Proyecto Epoz
http://epoz.sourceforge.net
Tim Bray: reinventando la rueda
http://www.tbray.org/ongoing
Herramientas para migración de información
http://www.developerfusion.com/show/4415
Manila
http://manila.userland.com/
COREBlog
http://www.coreblog.org
Zope
http://www.zope.org
Python
http://www.python.org
Introducción al seguimiento de información
http://www.movabletype.org/trackback/beginners
http://www.cruftbox.com/cruft/docs/trackback.html
Información sobre RSS
http://www.xml.com/pub/a/2002/12/18/dive-into-xml.html
http://www.webreference.com/authoring/languages/xml/rss/intro/2.html
Reuven M. Lerner
http://www.blog.lerner.co.il
Blog Express
http://blogexpress.com
Blogger
http://www.blogger.com

Lector de noticias gratis

Las formas de mantenerse actualizado con todas las novedades y noticias utilizando Internet evolucionan constantemente. Visitar un blog y refrescar el contenido si estamos a la espera de nuevas noticias ya no es necesario. Utilizando RSS (*Really Simple Sindication*), existe numerosas utilidades gratis para recibir solo la información que nos interesa de distintos lugares. Una de ellas es BlogExpress. Esta aplicación desarrollada en .NET nos permite recibir los titulares de los diarios, grupos de noticias e inclusive buscar actualizaciones en páginas web.

Google tambien tiene su blog

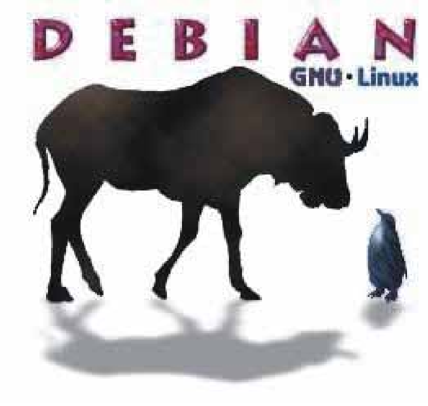
Asi es, como no podía ser de otra forma, el buscador mas utilizado también tiene su servicio de weblogs. Se llama Blogger y fue creado por Pyra Labs en 1999 y luego comprado por Google en el 2002.

Su uso es extremadamente sencillo e intuitivo, y permite automatizar el método para actualizar, modificar y subir los archivos como se necesita usualmente. Esto se logra utilizando un formulario al que podemos acceder luego de crear y configurar una cuenta en su sitio.

Las opciones de configuración son variadas, desde la elección de múltiples diseños hasta el tamaño y color de letra. Si poseemos conocimientos de HTML también nos es posible modificar manualmente el contenido

Todos los caminos llevan a Debian.

¿Por qué Debian? ¿Qué es Debian?



¿Qué es Debian?

Debian es una asociación de personas con un fin común, un proyecto iniciado hace más de 10 años orientado al desarrollo de un sistema operativo libre. ¿A que llamamos sistema operativo? A un conjunto de programas y utilidades básicas que brindan el funcionamiento de una computadora. El centro de un SO es el kernel (núcleo). En la actualidad Debian usa para su sistema operativo el kernel de Linux. Sin embargo se está trabajando para ofrecer Debian con otros kernels, concretamente el **núcleo Hurd**.

Obviamente, lo que la gente en su mayoría quiere es el software de aplicación, herramientas que lo ayuden, desde editar un documento a navegar en Internet. Debian incluye la mayor cantidad de software disponible para una distribución. Desde su sitio oficial (www.debian.org) podemos descargar (en su versión estable con 8710 **paquetes deb**) los 8 ISOs de la última **versión oficial** 3.0r2: **codename woody**.

Siendo en sus comienzos la distribución oficial de la **Free Software Foundation** (FSF) (www.fsf.org) en la actualidad mantiene una estrecha relación con la FSF por ser la distribución que respeta al pie de la letra el proyecto **GNU** (www.gnu.org). Por todo esto, y accediendo al pedido de la FSF, la distribución de Linux de Debian lleva el nombre **Debian GNU/Linux** y no solo Debian Linux por usar las herramientas GNU y el kernel de Linux.

debian

¿Qué ventajas tiene Debian?

- **Totalmente actualizable:** Debian es la única distribución que puede decir abiertamente que desde la versión 2.1 hasta la última el sistema se puede actualizar total y completamente sin perder ninguna de las funcionalidades actuales. Esto, en otras distribuciones es impracticable. Esto se debe principalmente al cuidado y control que se tiene sobre las aplicaciones que se desarrollan, al sistema de **paquetes deb** y a la aplicación que administra estos paquetes: el **apt-get**. En cualquier otra distribución, actualizar una versión a otra es impracticable, la única posibilidad es guardar los datos actuales e instalar desde cero para que todo quede realmente bien.

- **Arquitecturas que soporta:** La distribución completa se encuentra disponible para la mayoría de las arquitecturas conocidas, entre ellas todas las variantes de PC (intel, amd, cyrix, via), SUN SPARC, MK68K (atari, amiga y apple), ALPHA, POWERPC, MIPS (cobalt), ARM, HPPA (HP pa-risc), IA-64 (intel 64bits), S390 (IBM S/390 series). Por otro lado, esta casi terminada su disponibilidad para AMD64 para soportar los microprocesadores Opteron tanto en 32bits como en 64bits.

A su vez, el kernel de Linux no es el único disponible, también está en desarrollo **el kernel Hurd** (que es un desarrollo propio y libre de la FSF), el kernel de FreeBSD y NetBSD.

- **Debian es libre:** Hay un **contrato social** que se respeta a la hora de tomar decisiones. En muy resumidas cuentas, el contrato social asegura que Debian continuará siendo 100% libre por siempre, que todo el software desarrollado estará disponible para la comunidad, que no se ocultarán problemas y que todos los programas en la distribución tienen que cumplir el estándar de ser libres. Si bien existe la posibilidad de tener software que no cumpla este último requerimiento estarán disponibles en otras secciones llamadas **contrib** y **non-free** y no tienen que ser herramientas fundamentales para el sistema.

- **No existen los problemas de dependencias:** Debian utiliza el formato DEB y para instalar una aplicación sólo alcanza con un comando en consola. Podemos actualizar todo el equipo, instalar y desinstalar aplicaciones. El **apt-get** simplifica la administración de paquetes y nos hace olvidar de las dependencias que tantos problemas traen en distribuciones rpm. Sencillamente el sistema les avisará qué es lo que va a necesitar instalar para satisfacer las dependencias de la aplicación y procederá a conseguirlas. Si no tienen los CDs, sencillamente se conectará al mirror de Debian más cercano y se bajará lo que necesite. Todo totalmente compatible con lo que ya había instalado manteniendo una base de datos de lo instalado y lo disponible para instalar.

- **Se respeta el Filesystem Hierarchy Standard:** Este estándar determina la ubicación en el árbol de directorio de las aplicaciones y archivos de configuración y es respetado totalmente. Todos los archivos de configuración están en /etc. Las aplicaciones esenciales del administrador en /sbin, etc. De esta forma se garantiza la compatibilidad con otras distribuciones y sistemas Unix.

- **Fuentes:** Para toda aplicación existen sus fuentes y la posibilidad de instalarlas con la misma simpleza que con el "apt-get install aplication". También se pueden conseguir las fuentes e instalarlas personalizándolas de acuerdo con nuestras necesidades y aprovechando nuestro hardware como hace gentoo (www.gentoo.org) con su sistema de ports basado en FreeBSD.

- **Calidad y testeo:** El proyecto le presta más atención a la calidad y al testeo que al lanzamiento de nuevas versiones para que la gente las pruebe en sus equipos. Por esto es que no hay lanzamientos muy frecuentes dado que para que haya que generar una versión nueva de la distribución tiene que haber pasado un período en el cual se hayan testeado todas y cada una de las aplicaciones y no haya ningún bug (error) reportado. Esto lleva a tener una distribución robusta y probada, sin problemas ni agujeros de seguridad. Se utiliza el **Bug Tracking System** como base de datos para tener un control de los problemas reportados y su estado. La mayoría de los problemas son solucionados en días y todos están publicados en la página web.

- **Varias versiones en simultáneo:** A diferencia de otras distribuciones, para que una aplicación sea aceptada en la distribución tiene que haber cumplido cierto período de madurez, aparte de respetar los estándares. Para esto, existen tres versiones en simultáneo, **stable, testing y unstable**. La versión **stable** es la que se encuentra en la versión 3.0r2: codename woody y contiene los 8710 paquetes. En **stable** todas las aplicaciones están totalmente probadas. Por otro lado está la versión **testing (sarge)** que tiene muchas más aplicaciones en sus versiones mas recientes. Una aplicación se encuentra en período de prueba porque depende de alguna aplicación que esta todavía en **unstable (sid).** Las aplicaciones que se encuentran en **unstable** no están



más actuales que las de **testing** y **stable**. En **unstable** hay más de 12000 aplicaciones. Si bien las aplicaciones en unstable tienen errores o no están totalmente probadas, son igual de estables que cualquier distribución del mercado que anda por su versión 9. Personalmente uso la versión unstable hace tiempo para mi computadora sin mayores inconvenientes.

? **Disponible en varios idiomas:** No es una virtud exclusiva de Debian, cualquier distribución podría tener sus programas y manpages en varios idiomas. Pero Debian se encarga de mantener su distribución en los 13 idiomas mas usados, inclusive las manpages.

¿Quienes trabajan para Debian? ¿Que soporte hay disponible?

Con más de 1200 desarrolladores, respetando el **contrato social** de Debian, es la distribución con más gente colaborando. Cuando hablamos de colaboradores hacemos hincapié en el hecho de que Debian es un proyecto sin fines de lucro a diferencia de las "distribuciones.com". Una de las ventajas de esto es que Debian jamás cancelará el presupuesto para el desarrollo de su distribución Linux, nunca discontinuará la distribución libre para fomentar la venta de una versión enterprise, ni tampoco existe la posibilidad de que se tenga que presentar en quiebra. Sin embargo el no tener un soporte económico tiene varias desventajas, a saber:

? Al no existir la posibilidad de cerrar un trato económico, empresas como Oracle y Borland no certifican a Debian como una distribución soportada por ellos.

? No existe soporte oficial, ni siquiera durante los meses posteriores a la instalación como sí tienen las distribuciones.com.

Si bien esto en primera instancia aparenta ser un gran problema, a la hora de introducir a Debian en una empresa, tanto Oracle como Kylix, (el entorno de desarrollo de Delphi para Linux), funcionan sin inconvenientes. Mientras que Kylix, que sí está certificado para RedHat, tiene problemas en la instalación y solo funciona con versiones concretas de RedHat. En cuanto al soporte oficial, Debian es conocida por ser la distribución con mayor documentación disponible y por respetar todos y cada uno de los estándares. Cualquier empresa que brinde soporte para Linux debería tener la capacidad de dar soporte para Debian.

Algunas otras quejas comunes con Debian GNU/Linux.

El **dselect** es confuso para aprender: Es el frontend para la administración de paquetes en Debian. En la actualidad ya está superado y reemplazado por otros frontends como el **aptitude** para consola o el **synaptic** para modo gráfico. El problema concreto con el **dselect** es que cuando fue concebido no había semejante cantidad de paquetes disponibles y crea mucha confusión tener que seleccionar entre 12.000 paquetes en una aplicación como el **dselect**.

Falta **software comercial popular:** Es sabido que mucho software comercial no está disponible para Linux. Toda la suite de **Macromedia**, a excepción del reproductor para flash, de momento no esta disponible. Hay un proyecto concreto de **Macromedia** para portar sus aplicaciones a Linux. Hay suites de oficina completas como el OpenOffice, el Koffice o el GnomeOffice. Para los que trabajen con bases de datos, Debian ofrece tanto mySQL como postgreSQL y soporta SAP DB, Oracle, Informix, IBM DB2 y otros.

Otros productos comerciales están siendo desarrollados a medida que las empresas se dan cuenta del mercado que pierden por no introducir sus productos en Linux. Por ser libremente distribuible es difícil calcular con exactitud la cantidad de usuarios de Linux, pero se estima que unos 15 millones de usuarios tienen Linux como sistema operativo.

Linux es **difícil de configurar:** Esta es un área en la que se está trabajando activamente, mucha gente considera que Linux es más sencillo de instalar que Windows. Los periféricos como las impresoras, tienen configuraciones muy sencillas para quienes no tienen experiencia previa.

No todo el **hardware** esta soportado por Linux: Un hardware muy particular, muy raro, muy viejo o muy nuevo pueden llegar a tener problemas. Concretamente son aquellos en los que el fabricante sólo desarrolló el driver para Windows (muchos módems, por ejemplo). Igualmente en la mayoría de los casos existe algún hardware equivalente disponible para Linux. Algunos fabricantes directamente optan por no detallar las especificaciones técnicas del producto como para poder darle soporte. Esta es una área en la que se esta trabajando.

¿Quiénes usan Debian GNU/Linux? ¿Hay otras distribuciones basadas en Debian?

Luego de RedHat, es la distribución más utilizada en sitios de Internet, sólo en nuestro país es utilizado en las siguientes entidades:

- Sitio oficial Presidencia de la Nacion Argentina: *www.presidencia.gov.ar*
- Secretaria de medios de la Nacion: *www.medios.gov.ar*
- Universidad Nacional de Buenos Aires: *www.uba.ar*
- Gobierno de la Ciudad de Buenos Aires: www.buenosaires.gov.ar
- Movicom: *www.movicom.com.ar*
- LUGar: *www.linux.org.ar*

Por otro lado, el Ministerio de Educación utiliza un proyecto nacional llamado Ututo (www.ututo.org), una **distribución basada en Debian y Suse** para brindarles conectividad a las escuelas. De hecho hay varias distribuciones basadas en Debian. Desde la y

hasta la discontinuada Corel Linux. Sólo por mencionar algunas podemos nombrar a: Adamantix, DemoLinux, Gibraltar, Libranet, Lindows, Linex, Morphix, Progeny, Stormix, etc.

¿Debian es gratis?

Uno puede preguntarse: ¿por qué gastará la gente horas de su propio tiempo escribiendo software, empaquetándolo cuidadosamente, y luego regalándolo? Las respuestas son tan variadas como la gente que contribuye. A algunas personas les gusta ayudar a otras. Muchas escriben programas para aprender más acerca de las computadoras. Más y más personas están buscando la manera de evitar los precios inflados del software. Un grupo creciente contribuye como un agradecimiento por todo el excelente software libre y gratuito que ha recibido de otros. En las instituciones académicas muchos crean software libre para ayudar a obtener los resultados de sus investigaciones en un uso más amplio. Las empresas ayudan a mantener el software libre para poder observar cómo se desarrolla éste, ¡no hay una manera más rápida de obtener una nueva característica que implementarla uno mismo! Desde luego, muchos de nosotros sólo lo encontramos divertido.

Debian está tan comprometido con el software libre que este compromiso se encuentra formalizado en el **Contrato Social**. Aunque Debian cree en el software libre, existen casos en los que la gente quiere o necesita disponer de software que no es libre en sus máquinas. Siempre que sea posible, Debian respaldará esto. Hay un número creciente de paquetes que tienen como única misión instalar software que no es libre en un sistema Debian. Como por ejemplo el caso de las fuentes truetype de Microsoft. El paquete Debian sólo baja las fuentes libremente como cualquier otra persona del sitio de Microsoft y las instala. Sólo tenemos disponible para bajar del mirror Debian la herramienta para luego bajar las fuentes.

¿Gratis? ¡Pero los CDs y el ancho de banda cuestan dinero!

Uno podría estar preguntándose: si el software es gratuito, ¿por qué tengo que pagar a un vendedor por un CD, o pagar a un ISP (un proveedor de Internet) para descargarlo? Cuando compra un CD, está pagando por el tiempo de alguien, por la inversión hecha para crear los CDs , y el riesgo (en caso de que no los pueda vender todos). En otras palabras, está pagando por el medio físico usado para distribuir el software, no por el software en sí.

Cuando usamos el término «libre», nos referimos a la libertad del software, no a que tenga que ser gratuito (N. del T.: en inglés, «free» es sinónimo de «gratuito» y de «libre»). Puede leer más sobre en el sitio de la Free Software Foundation (www.fsf.org).

Hay algo que vale aclarar: es muy común cuando la gente va al sitio de Debian a bajarse los CDs, sorprenderse con que estén disponibles o en DVD o en CD (8 isos). **No hace falta bajar todos los CDS,** con tan solo tener el CD 1 (de 650MB o el CD de instalación por red (50MB aprox.) o alguno de los disquetes de instalación por red uno puede instalar lo que necesite via Internet y solo bajarse lo que va a usar.

La mayoría del software cuesta cientos de dólares. ¿Cómo es que Debian lo regala?

Una pregunta mejor es, ¿cómo hacen las compañías de software para venderlo a un precio tan alto? Crear software no es como hacer coches. **Una vez que se ha conseguido una copia del software, los costos de producción por hacer un millón más son mínimos**.

Mírelo de ésta otra forma: si usted tiene un surtido interminable de arena en su patio trasero, podría estar deseando regalar arena. Sin embargo, sería tonto pagar un camión para que se la lleve a otras personas. Usted los haría venir y que se la lleven ellos mismos (equivalente a obtenerla de la red) o ellos podrían pagar a alguien para que se la llevara hasta su puerta (equivalente a comprar un CD). Así es exactamente cómo opera Debian y el porqué de que la mayoría de los CDs sean tan económicos.

Debian no gana ningún dinero de la venta de CDs. A la vez, se necesita dinero para pagar gastos como el registro del dominio y el hardware. Por ello, le pedimos que compre a uno de los fabricantes de CDs que donan parte del dinero a Debian.

El apt-get:

Hay varias herramientas para administrar los paquetes en Debian, todas trabajan y comparten la información. Usar una herramienta o la otra no nos va a impedir cambiar de administrador. Son diferentes formas de instalar una aplicación y más que nada son gustos. La herramienta inicial de Debian era el **dpkg**, ahora es el **apt-get**. Tanto el dpkg como el apt-get trabajan por consola. Hay frontends o GUIs para trabajar tanto en consola como en modo gráfico, entre ellos el ya antiguo **dselect**, el **aptitude** (muy recomendado) o en modo grafico, el **synaptic**.

¿Cómo se instala y se desinstala una aplicación?





Para instalar una aplicación, está la forma sencilla, en la cual sabemos el nombre del paquete **apt-get install paquete** y existe otra forma, sin saber el nombre del paquete. En este caso necesitamos averiguarlo. Tenemos dos opciones: recurrir a packages.debian.org y buscar el paquete en los buscadores del sitio o usar el **apt-cache search nombre_de_la_aplicación**. Esto nos debería devolver nombres de paquetes. Luego sigue igual que la primera opción, **apt-get install paquete**.

A diferencia de una distribución RPM el apt-get calcula las dependencias y las resuelve automáticamente. Por otro lado nos ofrece software que estaría relacionado con el que queremos instalar y que sería prudente instalar. Hace falta aclarar que el apt-get sabe donde está el paquete. En otras palabras, no hace falta que tengamos que bajar nada de Internet ni tener los CDs, el apt-get sabe en qué mirror están los paquetes disponibles, los baja solo y los instala. Luego corre un mini wizard para configurarlo básicamente y tenerlo andando.

¿Cómo es este proceso en una distribución RPM?

Bueno, en una distribución rpm tenemos que, primero, conseguir el paquete. Para esto podemos incursionar en **rpmfind.net** a ver si encontramos algo que funcione, o buscar algo desactualizado en los CDs de instalación. Luego, quedaría hacer un **rpm -ivh paquete**. ¿Pero qué pasa? Este paquete necesita de otro paquete y el rpm no sabe dónde está. Así que volvemos a **rpmfind.net** o a buscar entre nuestros CDs a ver si encontramos ese paquete. ¡Lo conseguimos! Cuando vamos a instalarlo nos pide una librería que no tenemos, bueno... nuevamente a buscar la librería a **rpmfind.net** o a nuestro CD. Imagínense que esto es de nunca acabar.



¿Finalmente, como se desinstala algo? Fácil: **apt-get remove paquete**.

¿Cómo se actualiza el sistema?

Como ya mencionamos, el apt-get mantiene una base de datos de




los programas instalados y de los programas disponibles para instalar, con sus versiones. También comentamos que hay tres versiones en paralelo de Debian GNU/Linux.

Bueno, imaginemos que queremos actualizar nuestros paquetes instalados a la versión nueva que hay disponible en los mirrors de Debian.

Alcanza con hacer un:

apt-get update && apt-get upgrade y solo contestar **yes** cuando se nos pregunte si queremos actualizar el equipo. El apt-get se va a encargar de bajar las aplicaciones, actualizar los paquetes, preguntarnos si queremos guardar las configuraciones nuevas o reemplazarlas y de bajar y subir los servicios actualizados para que apliquen los cambios.

Entonces con Debian, ¿cómo haría para instalar el kde?

Para instalar el **kde** alcanza con hacer **apt-get install kde**. Nada más, el apt-get se va a encargar de todo. Esto en Debian es estándar con cualquier aplicación. **Los problemas de dependencias no existen en la versión estable.**

¿Cómo se configura el apt-get?

Para que el apt-get consiga las aplicaciones tenemos que definir dónde puede conseguirlas. El principal archivo de configuración para las fuentes de instalación es el archivo **/etc/apt/sources.list**. El apt-get tiene un frontend para su configuración, es el **apt-setup**. El **apt-setup** nos va a preguntar de dónde el apt-get va a conseguir sus paquetes. Podemos poner múltiples opciones, como cdrom, ftpserver, mirror de Debian, directorio, etc. Luego de haber definido todo, nos quedaría pendiente actualizar la base de datos, dado que agregamos más posibilidades desde dónde actualizar. Para esto utilizamos **apt-get update**. Esto nos actualiza la base de datos. No estaría mal hacer luego un **apt-get upgrade** porque como agregamos nuevos medios de instalación, es probable que alguno de estos medios tenga cosas nuevas en relación a lo que tenemos instalado.

Preguntas frecuentes.

¿Qué es HURD?

Hurd es una colección de servicios que se ejecutan sobre un micro núcleo para implementar las distintas funcionalidades. El Hurd es el kernel oficial del proyecto GNU. Debian es la única distribución que ofrece el kernel de Hurd en su sistema operativo. Actualmente está disponible para testearlo en el sitio oficial de Debian y es un proyecto en activo desarrollo. Inicialmente se desarrolló porque no había otro kernel disponible, el kernel de Linux todavía no existía y había un montón de herramientas GNU que no tenían sistema operativo. Luego cuando Linux se hizo popular comenzaron a usarse estas herramientas con el kernel de Linux y nació el sistema operativo GNU/Linux. Tiempo después, Debian GNU/Linux.

¿Qué son los nombres woody, sarge, sid?

Son los codename de las versiones que se mantienen de la distribución. Están tomados de la película Toy Story. Por ahora se han utilizado los siguientes nombres: buzz (Buzz Lightyear), rex (el tiranosaurio), bo (Bo Peep, la nenita que cuidaba a la oveja), hamm (el chanchito alcancía), slink (Slinky Dog, el perro de juguete), potato era, por supuesto, Mr. Potato, woody (el cowboy) y sarge (el sargento del ejercito de soldaditos de plástico).

Cada vez que una versión en testing es aprobada, pasa a ser la versión stable y el nombre que usaba pasa a stable. En su momento, woody fue testing y ahora es stable. Lo mismo va a pasar con sarge. La diferencia con sid es que siempre va a ser unstable. **Sid** era el nenito de la casa de al lado que rompía los juguetes :)

También existe un release más, **experimental**. En este release es donde las aplicaciones están disponibles en un principio y son paquetes que sencillamente fueron empaquetados en deb y jamás fueron probados. Es para gente que quiere estar muy a lo último.

Conclusión

En conclusión, el proyecto Debian nos ofrece un sistema operativo libre, robusto, plenamente probado, con un sistema de paquetes impecable y un equipo de desarrolladores dedicado a cumplir con los estándares GNU. Mientras que por otro lado nos deja abierta la posibilidad de otros sabores con versiones actuales en sus distribuciones testing y unstable. Como si eso fuera poco, tenemos disponible Debian para netbsd, freebsd y hurd.

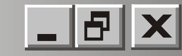
Guido Lorenzutti

Debianitas.net: Algo más que una página web

www.debianitas.net surgió de la idea de unos entusiastas usuarios del sistema operativo Debian GNU/Linux, al ver en los foros y chats la inmensa masa de gente a las que se le "atraganta" la configuración y puesta apunto de su equipo debido a que la mayoría de la documentación existente está en inglés. Debianitas.net intenta disponer la documentación adecuada, mediante la creación de manuales de fácil compresión, en castellano, que resuelvan las dudas más comunes para todos los usuarios.







Elementos básicos de criptografía

La criptografía es la ciencia que nos permite proteger nuestros datos utilizando una transformación matemática de modo de transformarlos en ilegibles. Algunos ejemplos de su utilización son:

- Cuando necesito enviar / recibir información de un modo seguro a través de una red (intranet, extranet ó internet) la "encriptación" (cifrado) es la herramienta fundamental para poder realizar la tarea.

- Si mi computadora es extraviada y quiero proteger la información almacenada allí.

¿Qué funciones de seguridad me permite realizar la encriptación?

Autenticación: permite a quien recibe un mensaje, estar seguro que quien lo envía es quien dice ser.

Confidencialidad: asegura que nadie leyó el mensaje desde que partió. Sólo el destinatario podrá leerlo.

Integridad: asegura que el mensaje no ha sido modificado

Para entender como lograr esto detallaremos tres conceptos básicos de criptografía:

A- Algoritmos hash en un sentido
B- Encriptación con llaves (keys, claves) simétricas: se utiliza una llave
C- Encriptación con llaves públicas y privadas: se utilizan dos llaves

En artículos posteriores desarrollaremos infraestructuras que se construyen sobre éstos. Ejemplos: Como firmar digitalmente un documento o cómo haríamos para intercambiar una llave secreta. El concepto que sigue entender, es la llamada Public Key Infrastructure (Infraestructura de llave pública) (PKI) que nos detalla las directivas, los estándares y el software que regulan o manipulan los certificados, y las llaves públicas y privadas. En la práctica, PKI hace referencia a un sistema de certificados digitales, entidades emisoras de certificados (CA) y otras entidades de registro que comprueban y autentican la validez de cada parte implicada en una transacción electrónica.

Hash

Un hash, también denominado valor hash o síntesis del mensaje, es un tipo de transformación de datos. Un hash es la conversión de determinados datos de cualquier tamaño, en un número de longitud fija no reversible, mediante la aplicación a los datos de una función matemática unidireccional denominada algoritmo hash. La longitud del valor hash resultante puede ser tan grande que las posibilidades de encontrar dos datos determinados que tengan el mismo valor hash son mínimas. Supongamos que quiero "hashear" el siguiente mensaje: "mi mamá". Quiero que el mensaje se resuma en un solo número (valor hash). Podría por ejemplo, asociar a cada carácter ASCII su número (ASCII code number) asociado

"m i <espacio> m a m a"

109 + 105 + 32 + 109 + 97 + 109 + 97 = 658.

Así el mensaje se "resumió" (digest) en un solo número. Notemos que ésta es una función en una dirección (no reversible). No hay manera de que alguien adivine el mensaje "mi mamá" a partir del 658 a menos que pruebe todos los posibles mensajes (infinitos) (y calcule sus "valor hash (digest)". Aún así tendría muchísimos con 658 y debería adivinar cuál es el correcto (imposible). Destacamos que la función (algoritmo) hash usada fue de lo más simple. En la vida real son usados algoritmos mucho más complejos. Podriamos por ejemplo, usar ese número para verificar si un mensaje enviado fue modificado en el camino: el remitente genera con un algoritmo un valor hash del mensaje, lo encripta y envía el hash encriptado junto con el mensaje. A continuación, el destinatario desencripta el hash, produce otro hash a partir del mensaje recibido y compara los dos hashes. Si son iguales, es muy probable que el mensaje se transmitiera intacto. Aquí supusimos que ambos conocen la llave para encriptar/desencriptar.

Funciones comunes de hash en un sentido

Las dos funciones hash siguientes son las más comunes:

MD5. MD5 es un algoritmo hash diseñado por Ron Rivest que produce un valor hash de 128 bits. El diseño de MD5 está optimizado para los procesadores Intel. Los elementos del algoritmo se han visto comprometidos, lo que explica su menor uso.

SHA-1. Al igual que el algoritmo de llaves públicas DSA, Secure Hash Algorithm-1 (SHA-1) fue diseñado por la NSA e incorporado por el NSIT en un FIPS para datos de hash. Produce un valor hash de 160 bits. SHA-1 es un conocido algoritmo hash de un sentido utilizado para crear firmas digitales.

FUNDAMENTOS DE SEGURIDAD INFORMATICA, PASO A PASO

Paso 1: Elementos Básicos de Criptografía

En este artículo expondremos:
>>¿Qué es criptografía?
>>Concepto de hash
>>Encriptación simétrica: una sola llave
>>Encriptación asimétrica: llave-publica y llave-privada
>>Entendiendo un algoritmo: El algoritmo RSA



Encriptación con llaves simétricas: una sola llave

La encriptación con llaves simétricas, es también denominada encriptación con llaves compartidas (shared keys) o criptografía de llave secreta (secret key). Se utiliza una única llave que posen tanto el remitente como el destinatario. La única llave que es usada (tanto para encriptar como desencriptar) se llama llave secreta (pero es también conocida como llave simétrica o llave de sesión). La encriptación con llaves simétricas es un método eficiente para el cifrado de grandes cantidades de datos.

Existen muchos algoritmos para la encriptación con llaves simétricas, pero todos tienen el mismo objetivo: la transformación reversible de texto sin formato (datos sin encriptar,



también denominado texto no encriptado) en texto encriptado.

El texto encriptado con una llave secreta es ininteligible para quien no tenga la llave para descifrarlo.Como la criptografía de claves simétricas utiliza la misma llave tanto para la encriptación como para desencriptar, la seguridad de este proceso depende de la posibilidad de que una persona no autorizada consiga la clave simétrica. Esta es la razón por la que también se denomina criptografía de clave secreta. Quienes deseen comunicarse mediante criptografía de claves simétricas deben encontrar algún mecanismo para intercambiar de forma segura la clave antes de intercambiar datos encriptados.

El criterio principal para valorar la calidad de un algoritmo simétrico es el tamaño de su llave. Cuanto mayor sea el tamaño de la llave, habrá que probar más combinaciones de diferentes llaves para encontrar la correcta que desencripte los datos.

Cuantas más claves sean necesarias, más difícil será romper el algoritmo. Con un buen algoritmo criptográfico y un tamaño adecuado de clave, es imposible, desde un punto de vista informático, que alguien invierta el proceso de transformación y obtenga el texto sin formato del texto encriptado en una cantidad de tiempo razonable.

Algoritmos de claves simétricas:

>**DES** (*Data Encryption Standard*): El DES nació como consecuencia del criptosistema Lucifer, creado por IBM. Este algoritmo cifra bloques de 64 bits mediante permutación y sustitución. Fue usado por el gobierno de los Estados Unidos hasta que se determinó que no era seguro.

>**3DES** (*Triple-DES*): La evolución del DES. Utilizando el Standard ANSI X9.52, este algoritmo encripta 3 veces la información y sigue siendo compatible con DES.

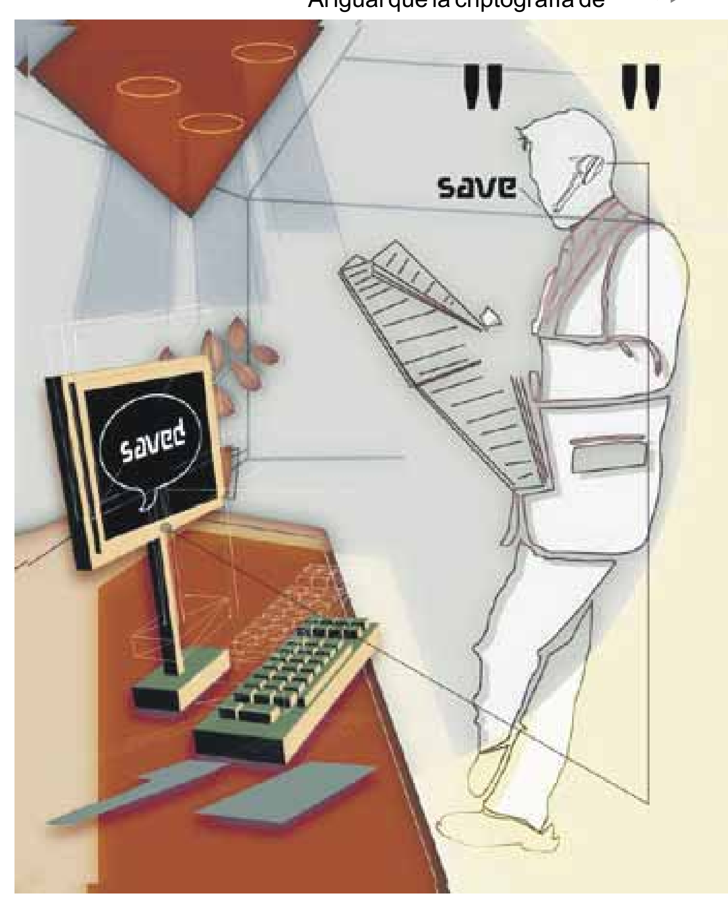
>**AES** (Advanced Encryption Standard): Ha sido un concurso abierto para analizar que algoritmo iba a reemplazar al DES. El 2 de octubre de 2000, el NIST anunció el algoritmo ganador: Rijndael, propuesto por los belgas Vincent Rijmen y Joan Daemen (de ahí su nombre). Rijndael es un cifrador de bloque que opera con bloques y claves de longitudes variables, que pueden ser especificadas independientemente a 128, 192 ó 256 bits

>**IDEA** (*International Data Encryption Algorithm*): Sistema criptográfico simétrico, creado en 1990 por Lai y Massey, que trabaja con bloques de texto de 64 bits, operando siempre con números de 16 bits. Este algoritmo es de libre difusión y no está sometido a ningún tipo de restricciones o permisos nacionales, por lo que se ha difundido ámpliamente, utilizándose en sistemas como UNIX y en programas de cifrado de correo como PGP.

Encriptación con llaves públicas: dos llaves (una pública y otra privada)

En la encriptación de llave pública (public key encryption) se utilizan dos llaves: una pública y una privada, que se encuentran relacionadas matemáticamente. Para diferenciarlo del cifrado de claves simétricas, en ocasiones el cifrado de claves públicas también se denomina encriptación con llaves asimétricas. En la encriptación de llaves públicas, la llave pública puede intercambiarse libremente entre las partes o publicarse en un repositorio público. Sin embargo, la llave privada será privada a quien cree el par (publico/privado). Los datos encriptados con la llave pública sólo pueden descifrarse con la llave privada. Los datos cifrados con la llave privada sólo pueden descifrarse con la llave pública.

Al igual que la criptografía de



llaves simétricas, la criptografía de llave pública también tiene diversos tipos de algoritmos. Sin embargo, el diseño de los algoritmosde llave simétrica y de llave pública es diferente. Puede sustituir un algoritmo simétrico por otro simétrico dentro de un programa sin cambios o con cambios mínimos, ya que ambos algoritmos funcionan de la misma manera. Por otro lado, los algoritmos de llave pública (que no son iguales) funcionan de manera muy diferente y, por tanto, no se pueden intercambiar.

Los algoritmos de llave pública son ecuaciones matemáticas complejas en las que se utilizan cifras muy altas. Su principal inconveniente es que proporcionan formas relativamente lentas de criptografía.En la práctica, se utilizan generalmente sólo en situaciones críticas, como en el intercambio de una llave simétrica entre entidades o para la firma de un hash de un mensaje. El uso de otras formas de criptografía, como la criptografía de llaves simétricas, junto con la criptografía de llaves públicas optimiza el rendimiento. La encriptación por llaves públicas proporciona un método eficiente para enviar a otra persona la llave secreta que se utilizó cuando se realizó una operación de encriptación simétrico sobre una gran cantidad de datos.

También puede combinar la encriptación con llaves públicas con algoritmos hash para producir una firma digital

Algoritmos típicos de claves públicas
Los tres algoritmos siguientes de llaves públicas son los que se utilizan con más frecuencia:

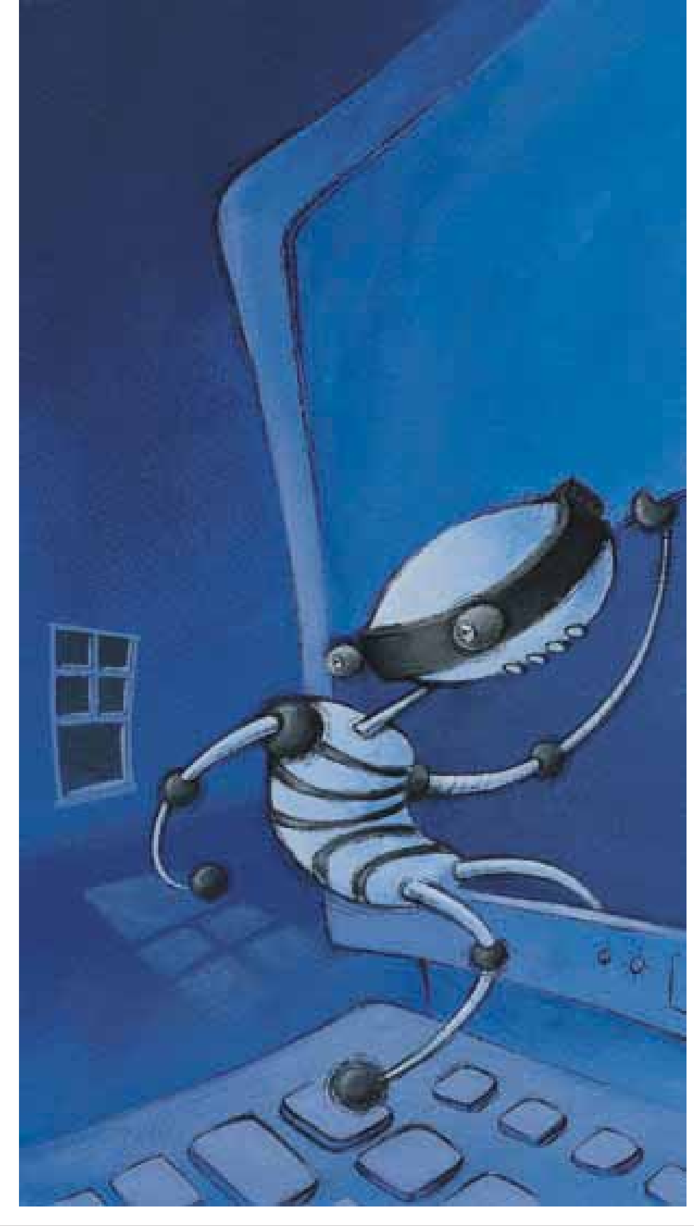
>**RSA**: para las firmas digitales y los intercambios de llaves. Hoy en día, los algoritmos criptográficos Rivest-Shamir-Adleman (RSA) son los algoritmos de llave pública más utilizados, especialmente para los datos que se envían a través de Internet. El algoritmo toma su nombre de sus tres inventores: Ron Rivest, Adi Shamir y Leonard Adleman. La seguridad del algoritmo RSA se basa en la dificultad (en términos de velocidad y tiempo de procesamiento) de comparación de números altos.

El algoritmo RSA es único entre los algoritmos de llaves públicas utilizados habitualmente ya que puede realizar operaciones tanto de firma digital como de intercambio de llaves. Los algoritmos criptográficos RSA son compatibles con Microsoft Base Cryptographic Service Provider (Microsoft Base CSP1) y con Microsoft Enhanced Cryptographic Service Provider (Microsoft Enhanced CSP2), y están integrados en numerosos productos software, incluido Microsoft Internet Explorer.

>**DSA**: únicamente para firmas digitales. El National Institute of Standards and Technology (NIST, Instituto Nacional de Estándares y Tecnología) de Estados Unidos incorporó el Algoritmo de firma digital (DSA), inventado por la National Security Agency (NSA, Agencia de Seguridad Nacional), al Federal Information Processing Standard (FIPS, Estándar Federal para el Procesamiento de Información) para firmas digitales. El DSA obtiene su nivel de seguridad de la dificultad para calcular logaritmos discretos. Este algoritmo sólo puede utilizarse para realizar operaciones de firma digital (no para la encriptación de datos). Microsoft CSP es compatible con el algoritmo DSA.

>**Diffie-Hellman**: únicamente para el intercambio de llaves. Diffie-Hellman, el primer algoritmo de llaves públicas, recibió el nombre de sus inventores Whitfield Diffie y Martin Hellman. Diffie-Hellman obtiene su nivel de seguridad de la dificultad para calcular logaritmos discretos en un campo finito. El algoritmo Diffie-Hellman puede utilizarse únicamente para el intercambio de llaves. Microsoft Base DSS3 y Diffie-Hellman CSP son compatibles.

Juan Manuel Zolezzi



Explicación matemática del algoritmo RSA

El sistema RSA se basa en la dificultad de factorizar números muy grandes. Para factorizar un número el sistema más común consiste en empezar a dividir sucesivamente éste entre 2, entre 3, entre 4,..., y así sucesivamente, buscando que el resultado de la división sea exacto, es decir, de resto 0, con lo que ya tendremos un divisor del número. Si el número considerado es un número primo (el que sólo es divisible por 1 y por él mismo), para factorizarlo habría que empezar por 1, 2, 3,… hasta llegar a él mismo, ya que por ser primo, ninguno de los números anteriores es divisor suyo. Y si el número primo es lo suficientemente grande, el proceso de factorización es complicado y lleva mucho tiempo. Basado en la exponenciación modular de exponente y módulo fijos, el sistema RSA crea sus claves de la siguiente forma:

1. Se buscan dos números primos lo suficientemente grandes: **p** y **q** (de entre 100 y 300 dígitos).
2. Se obtienen los números **n** = p * q y **Ø** = (p-1) * (q-1).
3. Se busca un número **e** tal que no tenga múltiplos comunes con Ø.
4. Se calcula **d** = e^{-1} mod Ø, con mod = resto de la división de números enteros.

Y ya con estos números obtenidos, **n es la clave pública y d es la clave privada**. Los números p, q y Ø se destruyen. También se hace público el número e, necesario para alimentar el algoritmo.

El cálculo de estas claves se realiza en secreto en la máquina en la que se va a guardar la clave privada, y una vez generada ésta conviene protegerla mediante un algoritmo criptográfico simétrico.

En cuanto a las longitudes de claves, el sistema RSA permite longitudes variables, siendo aconsejable actualmente el uso de claves de no menos de 1024 bits (se han roto claves de hasta 512 bits, aunque se necesitaron más de 5 meses y casi 300 ordenadores trabajando juntos para hacerlo).

RSA basa su seguridad en ser una función computacionelmente segura, ya que si bien realizar la exponenciación modular es fácil, su operación inversa, la extracción de raíces de módulo Ø no es factible a menos que se conozca la factorización de e, clave privada del sistema.



Windows Longhorn



La evolución de Windows XP, conocida con el nombre clave Longhorn, no saldrá a la venta hasta el 2006, pero el desarrollo está en pleno proceso. A

"El lanzamiento del sistema operativo mas importante desde Windows 95"

Las claves de Longhorn

Longhorn se enmarca dentro de la apuesta de Microsoft por incrementar la seguridad, el rendimiento, la conectividad y la escalabilidad de los sistemas informáticos. El nuevo Windows extenderá las actuales tecnologías de seguridad en Windows XP contra peligros externos, y presentará nuevas mejoras en el nivel de la arquitectura, que podrá ser utilizada por los desarrolladores para obtener aplicaciones y servicios más seguros. Éstas son las claves del nuevo modelo:

- **WinFS** (*Windows Future Storage*): Esta es sin duda, una de las características más importantes del nuevo sistema operativo. Se trata de la próxima generación de almacenamiento de datos: facilita la forma de encontrar, relacionar y actuar sobre la información. Gracias a WinFS se pueden almacenar de forma segura datos estructurados y no estructurados. Además, con WinFS los desarrolladores podrán utilizar estructuras de información preconstruidas en bases de datos, utilizando una nueva versión de Microsoft SQL, Yukon.

En WinFS la información se organiza independientemente de como esté archivada físicamente. La manera cómo los usuarios y aplicaciones organizan esta información, también está separada de cómo se almacena en el disco. Para beneficiar a los desarrolladores, WinFS soporta servicios de datos unificados para todas las aplicaciones de usuario final. Servicios integrados de datos, como la sincronización, notificación, un almacenamiento unificado y un modelo común de seguridad, así como su integración con otras tecnologías como redes punto a punto (P2P) y servicios de directorio, hacen que los datos se compartan más fácilmente. Estos servicios le permiten escribir aplicaciones que intercambian datos con aplicaciones realizadas por otros desarrolladores. Igualmente, WinFS trabaja con otras tecnologías basadas en Windows para permitir compartir información remotamente con otros WinFS o no-WinFS.

- **Avalon**: Es el subsistema gráfico de Windows Longhorn. Facilitará una arquitectura unificada para presentar la interfaz de usuario, los documentos y los elementos multimedia. Avalon permitirá a los desarrolladores sacar provecho fácilmente del hardware gráfico y proveer un soporte nativo para la programación que simplifique la construcción de aplicaciones basadas en .NET.

Una de las motivaciones para crear este nuevo sistema gráfico surge a partir de la idea de aprovechar la nueva potencialidad de las tarjetas de video actuales.

Al incluir Avalon, se aumenta la capacidad gráfica e incrementa la velocidad de procesamiento de video gracias al soporte de doble buffer. Conjugado con un nuevo lenguaje de definición de pantallas llamado XAML (*Extensibility Application Markup Language*), Microsoft ha logrado separar por completo la definición de la interfaz de usuario del código asociado a ella.



- **Indigo**: Enfatiza el esquema de comunicaciones de Windows al trabajar con protocolos basados en XAML. Indigo incluirá implementaciones de protocolos de servicios Web que actualmente están en desarrollo, incluido un sistema de transacciones y mensajería fiable. Construido con .NET Framework, permite crear aplicaciones orientadas a servicios. En un futuro, se prevee el soporte de Indigo para Windows 2003 y XP.

Más funciones

A nadie le sorprenderá la incorporación de .NET Framework, eliminando así la necesidad de bajar e instalarlo por separado. De esta forma, Microsoft termina de estandarizar el nuevo lenguaje para el desarrollo e implementación de software.

Ahora con Longhorn, la lista de contactos la maneja y administra el mismo SO, sin necesidad de una aplicación por separado como Microsoft Outlook. Esta utilidad utiliza el nuevo sistema de archivos WinFS.

Otro detalle muy importante de Windows Longhorn será la seguridad. En enero del 2001 Bill Gates comenzó una nueva iniciativa orientada a no poner tanto interés en las nuevas características del software en favor de evitar los bugs y mejorar la seguridad.

Palladium es el nuevo estándar de seguridad a ser incluido en Longhorn. Entre otras cosas, este sistema informará con quién estás tratando "online" y qué está haciendo, y necesitará chips especiales que constituyen un hardware de seguridad. Estas y muchas de las funciones que incluye Palladium, son hechas para proteger a los usuarios de virus o códigos malintencionados, pero muchos lo critican severamente, debido a que toda la información estará bajo el control del sistema, regulando qué datos se pueden copiar y/o ver y cuáles no.

Datos curiosos

Aparte de la necesidad de una CPU y memoria de video localizada, otra de las necesidades básicas del nuevo SO es una lectora de DVD. Así es, Microsoft no hará Longhorn disponible en CD-ROM debido al inmenso tamaño que requiere; más de 5GB si sumamos el "development kit" (SDK) en las versiones para 64-bit y 32-bit.

En vez de suministrar una "product id", Microsoft exige al usuario a loguearse en un website seguro.

El ID y el password están asociados con una PC. Luego de ser instalado el "product key", deberá ser activado dentro de los 14 días.

Los requerimientos por supuesto son mucho mayores a los del Windows 2003 o XP. Los usuarios finales necesitarán un mínimo de 256 MB y un procesador de 800MHZ, mientras que para los desarrolladores se recomienda 1GB de RAM, y un procesador de 1.6GHZ.

Ambos necesitan de una placa de video con 32MB y 64MB de memoria de video, debido a Avalon, el cual demostró que por ahora, si uno no dispone de dicha placa, el rendimiento se verá severamente afectado.

La versión pre-beta no soporta la actualización de una instalación de Windows existente, con lo cual una instalación limpia es por ahora la única opción.

Conclusiones

Mejoras en la interfaz de usuario, gestores de información más potentes y nuevas posibilidades para diseñar una estructura orientada a servicios: la nueva versión de Windows promete revolucionar a toda la comunidad internacional de IT. Los primeros pasos ya están dados.

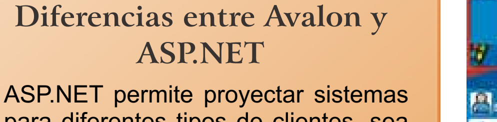
Pablo Fernícola, Program Manager del equipo de Avalon, aconseja aprender y entender bien Windows Forms y .NET, ya que nos "obliga" a realizar la separación entre lo visual y la lógica, lo cual asegura una buena base para luego poder saltar a LongHorn y Avalon.

Link de interés:

>http://www.longhornblogs.com

>http://msdn.microsoft.com/longhorn/

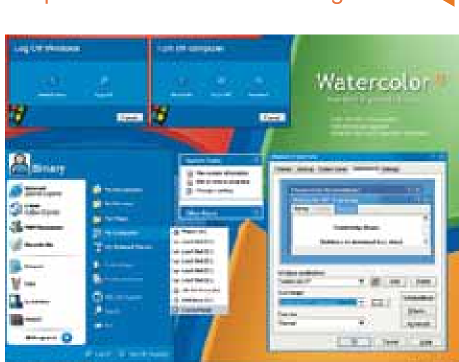
Juan Manuel Zolezzi



Diferencias entre Avalon y ASP.NET

ASP.NET permite proyectar sistemas para diferentes tipos de clientes, sea Windows 95, o simplemente HTML básico, de manera de que todos los clientes puedan acceder a la funcionalidad de la aplicación. Pero como necesita ser común a diferentes clientes, debe presentar lo mínimo de funcionalidad posible.

Cuando se quiere hacer algo que sea más interactivo, que permita al usuario trabajar con los documentos de su PC o gráficos de interacción, es el caso de usar un modelo basado en el cliente, ya sea Windows Forms hoy en día o Avalon en un futuro. En términos de programación, hay aspectos similares entre los dos: el uso del código manejado, y la separación de la parte lógica de la visual.







LongHorn y Blackcomb

Windows LongHorn aparecerá durante el año 2006, y será una versión para el hogar o estaciones de trabajo, en otras palabras, el sucesor directo de Windows XP. La versión para servidores, conocida como Windows Blackcomb, saldrá algunos años después que LongHorn. Estas fechas de lanzamiento dependen directamente el Departamento de Justicia de Estados Unidos y sus querellas legales a favor del antimonopolio de Microsoft. Este Windows Blackcomb es el sucesor directo de Windows Server 2003, y un rumor informa que verá la luz poco después del 2006.

openMosix y Condor

Soluciones libres al problema del load-balancing en clusters

En este artículo el Dr. Reinaldo Pis Diez explica los tipos de clusters que existen y cómo openMosix y Condor nos proveen una solución al problema de "load balancing" (balance de carga). En un artículo previo en NEX2 [2] explicó claramente como implementar un cluster "beowulf" usados fundamentalmente en High Performance computing (HPC).

Uno de los objetivos del *clustering* es distribuir eficientemente entre los componentes del cluster, fundamentalmente entre aquellos que se encuentran libres, la carga ocasionada por los requerimientos de los usuarios.

Se acepta en la actualidad que existen tres tipos de clusters [1]:

1. Cluster «a prueba de fallas» es aquel conformado por dos o más máquinas conectadas en red de forma tal que constantemente se controla la actividad de todos los servicios prestados. En cuanto un servicio en una máquina se detiene por cualquier causa, otro componente del cluster intenta reemplazarlo inmediatamente. Esta configuración se conoce también como «redundancia».
2. En un cluster con balance de carga los requerimientos entrantes son enviados al componente más aliviado del mismo. Un cluster de este tipo es también un cluster a prueba de fallas, sólo que con un mecanismo de balance de carga activado.
3. Un cluster para computación de alto rendimiento, también conocido como «Beowulf» [2], es diseñado para soportar los importantes requerimientos de cálculo numérico de centros de investigación. También posee mecanismos de balance de carga y soporta entornos de programación especiales que permiten procesar información en paralelo.

En términos del tipo de tareas a desarrollar, un cluster puede ser clasificado según los siguientes criterios:

1. Las tareas que implican el manejo de una gran cantidad de datos durante un prolongado período de tiempo se denominan genéricamente «computación de alta producción» (High-Throughput Computing o HTC) y requieren de un cluster HTC.
2. Las tareas que requieren inmensos recursos computacionales en tiempos relativamente más cortos se definen como «computación de alto rendimiento» (High-Performance Computing o HPC) y requerirán un cluster HPC.

Los inicios de la tecnología Mosix se remontan a los comienzos de la década de 1980. Hacia 1997, y debido a un rumbo netamente comercial tomado por los desarrolladores de Mosix, Moshe Bar decide llevar a cabo el proyecto openMosix bajo licencia GPL2.

openMosix es un parche a nivel del kernel de Linux compatible con plataformas de tipo IA32 [3]. Un sofisticado algoritmo basado en premisas de la economía de mercado es utilizado para determinar cuál nodo es el indicado para transferirle un proceso de forma de optimizar el balance de carga total del cluster.

openMosix tiene un importante conjunto de herramientas de configuración, incluyendo la interfaz gráfica dada por openMosixview [4] que simplifica notablemente la administración de un cluster.



Una interesante característica de openMosix es la denominada «autodiscovery» que permite detectar nuevos nodos en un cluster y actualizar automáticamente la configuración del mismo para reflejar los cambios producidos.

A diferencia de un cluster Beowulf, donde lo usual es ejecutar procesos de larga duración, openMosix es particularmente útil en sitios donde los usuarios deben llevar a cabo múltiples instancias relativamente rápidas de uno o más programas. Sin embargo, aplicaciones en paralelo bajo Message Passing Interface, MPI [5], pueden perfectamente llevarse a cabo en un cluster openMosix: si un subproceso es iniciado en el nodo 1 y en determinado momento el nodo 2 presenta menor carga, entonces el subproceso es migrado a este último nodo de una forma que resulta totalmente transparente al usuario.

Condor es un sistema de administración inicialmente diseñado para HTC, donde lo esencial es que el proceso finalice felizmente dado el gran tiempo de cálculo necesario [6].

Al igual que openMosix, no es necesario modificar los programas existentes para poder utilizarlos en un cluster administrado por Condor. Sin embargo, si es posible reconstruir el o los ejecutables aprovechando un conjunto de funciones de biblioteca de Condor, entonces dos importantes ventajas salen a la luz: la generación de «checkpoints» y llamadas de sistema remotas.

Un checkpoint es un archivo que contiene la información completa del estado de un proceso. De esta manera, cuando ocurre un corte de luz o la computadora debe ser reiniciada por alguna razón, el proceso es relanzado desde el último estado registrado en el archivo checkpoint.




Por otro lado, cuando el nodo en el que originalmente es iniciado un proceso sale temporariamente de servicio, Condor puede migrar a otro componente del cluster tanto el proceso como el archivo checkpoint asociado para continuar la tarea.Cuando un proceso es iniciado por un usuario en un componente dado de un cluster, Condor puede migrarlo a otro nodo (nodo remoto) pero mantener los archivos de entrada y salida en el nodo original. De esta forma, es Condor quien se encarga de las llamadas remotas al sistema en lugar del sistema operativo del nodo remoto. Una notable ventaja de este mecanismo es que el usuario ni siquiera necesita una cuenta en el nodo remoto ya que es Condor quien se encarga de todo el proceso.

Condor es extremadamente flexible en su configuración, permitiendo incluso que computadoras de escritorio formen parte de un cluster pero sólo a partir de las 18 horas de cada día y hasta las 8 de la mañana del día siguiente y durante la totalidad de los fines de semana.

Clusters: un poco de historia

- Décadas del 50 y 60: la Fuerza Aérea norteamericana construye una red de computadoras (funcionando con válvulas) como método de defensa contra un eventual ataque nuclear de la entonces Unión Soviética. Denominaron a esa red SAGE .
- Mediados del 80, la Digital Equipment Corporation acuñó el término «cluster» para bautizar su sistema de minicomputadoras VAX
- Comienzos de los 90: bajo costo de PCs , rápido desarrollo de la tecnología Ethernet y la aparición de Linux permite usar las PCs como «unidades de construcción» de un cluster.
- 1994: El Centro Espacial Goddard de la NASA presentó un cluster de 16 PCs, (usando procesador Intel486 bajo Linux). Potencia máxima de cálculo de 70 megaflops (1 megaflop = 1 millón de operaciones de punto flotante por segundo), similar a la brindada por sistemas comerciales cuyo valor era de 10 veces superior. Denominaron al cluster «Beowulf», en honor del rey anglosajón del medioevo que derrotó al monstruo Grendel arrancándole un brazo.
- A diez años del nacimiento del cluster Beowulf, en la actualidad es posible verificar la presencia en el puesto 5º del Top500 de un cluster de PCs basado en 1920 procesadores Intel Xeon de 2.4 GHz, situado en el Lawrence Livermore National Laboratory de los Estados Unidos, el cual alcanza casi 6 TFlops de rendimiento sobre un pico teórico de 9.2

Habiendo reseñado las principales características de openMosix y Condor, haremos algunas observaciones que deberían aclarar la verdadera utilidad de estos dos productos.

Básicamente, tanto openMosix como Condor son «administradores de colas». Ninguno de los dos ofrece un entorno de programación en paralelo. Para ello, es necesario utilizar Parallel Virtual Machine, PVM [7], o el ya mencionado MPI, e introducir las modificaciones al software original como llamadas a funciones de biblioteca de aquellos. Ni openMosix ni Condor pueden reemplazar estas utilidades.

Se suele indicar que no es necesario recompilar un programa si se instala openMosix o Condor en un cluster. Esto es cierto para cualquier administrador de colas, no sólo para los productos que se discuten en este artículo. Por otro lado, si un programa es paralelizado, usando por ejemplo las funciones provistas por MPI, entonces el ejecutable deberá reconstruirse independientemente de la naturaleza del administrador de colas instalado en el cluster. Ni openMosix ni Condor pueden evitar la recompilación de la versión paralelizada del programa original.

Se cita también como una ventaja de estos productos que cuando un usuario ejecuta un programa, puede olvidarse del camino que seguirá el mismo hasta ser notificado de su finalización.

En realidad, cualquier administrador de colas efectúa esta tarea y no es una característica única de openMosix ni de Condor.

Para finalizar, digamos que tanto openMosix como Condor son dos excelentes productos que pueden funcionar muy bien como una solución al problema del balance de carga en clusters para HTC o HPC.

No obstante, no debe perderse de vista que son fundamentalmente administradores de cola inteligentes que no proveen por sí mismos un entorno de programación o de trabajo en paralelo aunque sí son capaces de llevar a cabo procesos que se reparten entre varios nodos.

[1] "Introducing openMosix", K. Buytaert. http://www.linuxdevcenter.com/pub/a/linux/2004/02/19/openmosix.html.

[2] "High Performance Computing a un costo reducido Clusters Beowulf bajo Linux", R. Pis Diez, Nex Periódico de Networking, No. 2, 2003. http://www.nexweb.com.ar/e_anteriores/nex_2/linux/nota1.asp

[3] http://openmosix.sourceforge.net/

[4] http://www.openmosixview.com/

[5] http://www-unix.mcs.anl.gov/mpi/mpich/

[6] http://www.wisc.edu/condor/

[7] http://www.csm.ornl.gov/pvm/

Autor: Dr. Reinaldo Pis Diez

Salida Laboral

Otra alternativa: El Servicio de Empleo de la AMIA

AMIA
Servicio de Empleo



Desde hace más de 30 años la AMIA (Asociación Mutual Israelita de Argentina) brinda un servicio de empleo de forma no lucrativa, que desde 1995 se ha extendido haciendo posible que cualquier persona se acerque para desarrollarse o reinsertarse profesionalmente en la sociedad. El Servicio de Empleo de AMIA surgió como una bolsa de trabajo en el año 1974, como una dependencia del Área de Acción Social. El objetivo era otorgar la oportunidad de obtener un empleo a quienes se acercaban a buscar ayuda, priorizando la posibilidad de brindar la posibilidad de conseguir su propio sustento en vez de otorgar un pequeño subsidio.

En 1998, el Gobierno Nacional la declaró la "Red de Trabajo no Privada Más Grande del País". Gracias a la colaboración de cientos de voluntarios con un alto grado de compromiso social se logró un éxito que fue valorado por el B.I.D. (Banco Interamericano de Desarrollo) con quienes firmaron un acuerdo de cofinanciamiento para la creación de una Red de Oficinas de Empleo que ampliará los servicios para empresas y postulantes, a fin de ayudarlos a reducir el impacto de la crisis económica argentina. Este importante apoyo fue el punto de impulso hacia lo que hoy es el servicio gratuito de empleo de mayor crecimiento en los últimos meses, con 7 sucursales en todo el país, y con un software propio para la administración de postulantes y empresas. Este software, llamado Verificador Inteligente de Perfiles, de Focus Pro-Search®, está desarrollado íntegramente en ASP que administra los datos de 2500 empresas en una base de datos de SQL Server 2000, y conecta las diferentes sucursales o "nodos", haciendo que la información compartida esté permanentemente actualizada. De esta manera, los postulantes de la provincia de Córdoba pueden postularse a un trabajo en La Plata si es que planean mudarse a esta zona. A su vez, la actualización al instante les garantiza que no se estarán postulando a puestos ya cubiertos.

Quienes están en la búsqueda laboral conocen esto y saben lo frustrante que a veces es postularse a muchos puestos de trabajo sin obtener ninguna respuesta, y encuentran en este sistema la posibilidad de aplicar los filtros necesarios para no recibir "SPAM" con oportunidades laborales no aplicables a su perfil. El servicio de empleo de la AMIA ofrece la posibilidad de suscribirse a un newsletter, que a diferencia de muchos otros, no entrega una "lista sábana" de oportunidades laborales que no concuerdan con su perfil, sino que los mantiene informados de las novedades del mercado al que apuntan y los cursos y talleres de capacitación de los que pueden participar. Esto garantiza una actitud activa por parte del postulante en su búsqueda laboral.

Los talleres que se ofrecen son muy amplios, abarcan asignaturas que van desde cursos de idioma, manejo de PC hasta de administración de consorcios y actividades para emprendedores, y están a cargo de consultores cuya tarea es la capacitación, evaluación y orientación del postulante. Además de estos talleres, el postulante puede participar de otras actividades, como el "Club de Empleo", donde se reúnen a compartir consejos, experiencias y datos importantes, y el "Cyber-Empleo" donde pueden, al disponer de una PC con conexión a Internet, crear o actualizar su Currículum Vitae, ingresarlo a la base de datos de postulantes e incluso imprimirlo para una entrevista laboral o para acercarlo a una empresa que necesite un empleado con su perfil.

Este servicio trabaja con postulantes para mandos medios (jefaturas, supervisión) hacia abajo: cargos operativos, de administración, atención al cliente, etc., y a quienes no tienen PC o los conocimientos necesarios para utilizarlas en el "Cyber-Empleo", se les ofrece la posibilidad de postularse llenando un formulario en papel que luego un voluntario cargará en la base de datos. Además, al momento de inscribirse, se les obsequia el "Directorio de Recursos Humanos" donde se detallan las direcciones y teléfonos de todas las consultoras de RRHH, de Personal Temporario, grandes empresas, sites de RRHH de argentina y del exterior, bolsas de trabajo y servicios de empleo



En cuanto al servicio para empresas, este servicio incluye el relevamiento del perfil del puesto en la empresa, reclutamiento de candidatos (a través del Focus Pro Search® y otras fuentes), entrevistas personales con los postulantes y el armado de una terna final para entrevistas con el cliente. Con la incorporación del candidato brindan además una garantía de entre 30 y 60 días por el postulante. También se ofrecen estudios previos a la incorporación (referencias, evaluación psicológica, socio-ambiental, etc.). Este servicio tiene un costo, que en general es el 50% del valor que normalmente cobran las consultoras de RRHH, ya que cuenta con el cofinanciamiento del BID. Resulta sumamente útil en el caso de que no cuente con el tiempo para citar, recibir y entrevistar gran cantidad de postulantes, y que quiera recibir un servicio del nivel de una consultora de RRHH a un costo mucho más accesible. Estos importantes servicios han sido utilizados por empresas como 5 a Sec, Librería Jenny, La Cardeuse, Jean Cartier, Origenes AFJP SA, Mercado Libre.com S.A, Fargo, Garbarino, Wall Street Institute, entre otras.

COR Technologies, como muchas otras empresas que apoyan e incentivan la capacitación en IT, aconseja a sus alumnos certificados, la inclusión en el sistema de empleos de la AMIA al momento de la búsqueda laboral.

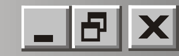
María Luján Zito

Agradecemos a Claudia Flores la información brindada.

¿Dónde más buscar trabajo?

Estos son los sitios de consultoras y bolsas de trabajo del país, una ayuda más que les brindamos en la búsqueda laboral.

www.trabajosnet.com
www.empleos.amia.org.ar
www.bumeran.com.ar
www.empleos.clarin.com.ar
www.clasificados.lanacion.com.ar
www.empleosweb.com.ar
www.cvempleos.com.ar
www.planetamedico.com/oportunidades/empleos
www.buscarempleos.com.ar
www.laborum.com
www.segundamano.com
www.empleovirtual2000.com.ar
www.recursosenlaweb.com.ar
www.empleosweb.com.ar
www.enlaces.qcom
www.execuzone.com
www.weblaboral1.com
www.empleos.amia.org.ar
www.gov.ar/teletrabajar
www.portalrh.com.ar
www.portalprofesional.com.ar
www.busquedasrh.com.ar
www.jobmarket.com.ar
www.cuvitae.com.ar
www.latpro.com.ar
www.trabajando.com
www.azcarreras.com.ar

ETHICAL HACKING PASO A PASO

Ethical Hacking Paso a Paso estará compuesto por una serie de artículos, expuestos mes a mes, básicamente sobre "las herramientas" de hacking y las contramedidas (countermeasures). Para cada acción de hacking existen diversas herramientas. Algunas de ellas engloban ya varias acciones, lo que las hace muy completas y poderosas. Nosotros detallaremos aquellas más populares y/o que consideremos excelentes para ejemplificar una dada acción.

ETHICAL HACKING
PASO A PASO
Paso1: Footprinting

En otra serie de artículos, desarrollamos un Paso a Paso de "Fundamentos de seguridad Informática" (ver Págs. 11-13 de este ejemplar) que se complementa con éste de hacking.

Pero antes de empezar, entendamos porque es importante conocer estas herramientas.

Describamos el esquema de la Figura 1. Nos muestra una empresa con dos firewalls back-to-back y una DMZ (Demilitarized Zone-Zona Desmilitarizada, donde ubicamos, por ejemplo, nuestros web-server, DNS, ftp-server, etc. Es decir servidores expuestos al mundo), un hogar y una nube (Internet). Pero qué representa esa nube?. Si incluyésemos en ese esquema más hogares y más empresas a miles o millones obtenemos lo que se llama Internet, o sea la nube. Los elementos que componen la llamada red-de-redes (Internet), son dispositivos (hardware: CPUs, hubs, switches, firewalls, routers y otros), conexiones (por ejemplo: cables UTP, antenas para wireless, fibra óptica), programas (sistemas operativos como Linux, Windows, Unix, Netware y aplicaciones como Office, Dreamweaver, The Gimp) y personas.

Las personas interactuando con los dispositivos, conforman una comunidad. Dentro de esa comunidad existen buenos y malos.

El término **"hacker"** nació asociado a los entusiastas de la computación interesados en aprender sobre los lenguajes de computación y los sistemas de cómputo. Estudiando los programas, detectando los errores de programación (**bugs o flaws**) e individualizando aquellos que permiten obtener privilegios a partes del sistema a los cuales no se está autorizado, detectan las **"vulnerabilidades"**.

Y, tan pronto un hacker descubre o alguien anuncia una vulnerabilidad, aparece el **"exploit"** (herramienta que se aprovecha de esa vulnerabilidad). Hoy el término se refiere a individuos que ganan acceso no-autorizado a sistemas de cómputo con el propósito de robar o corromper información. Los hackers mantienen que el nombre apropiado sería "**cracker**".

Asi, hoy se dice: hackeo un sistema (una computadora), hackeo una red (aprovecho un firewall mal configurado, hackeo un web-server (aprovecho una vulnerabilidad de Apache o el IIS).

El fin de algunos hackers es decir: "lo hice". Dejan una marca o evidencia mostrando su habilidad. Para otros el fin es dañar: cometer algún delito fraudulento o simplemente destruir.

El hacking solía ser tarea de unos pocos expertos muy capacitados. Hoy, existen un sin número de herramientas pre-hechas con las que solo hace falta apuntar a nuestro "target" (objetivo) y hacer clic. Son herramientas de destrucción muy poderosas capaces de causar mucho daño a nuestra "cyber-comunidad".

¿Cómo hacemos entonces para protegernos de los Hackers?

La respuesta es conocer. Para poder mejorar la seguridad y protegernos debemos conocer bien las modalidades usadas por los hackers. Los hackers cuentan con innumerables herramientas y metodologías que no podemos desconocer.

Ellos, debido a su naturaleza se reinventan continuamente y a sus técnicas.

El profesional de seguridad deberá por tanto conocer muy profundamente el ámbito de ataque y la filosofía de los atacantes de modo de poder ayudar a las empresas respecto de su seguridad. Deberá crear medidas concretas haciendo la infraestructura IT de las empresas menos vulnerables.

En los últimos años ha aparecido el concepto de "**ethical hacking**". Este, es alguien, quien dotado de las mismas herramientas que el hacker las utiliza para testear (penetration testing- test de penetración) nuestra red. Su expertise es tal que realizando tal test puede darnos el panorama de cuales son nuestras debilidades al poner nuestra empresa conectada en una intranet o a Internet.

Nota: es muy importante saber que 50% de los eventos de seguridad provienen de nuestras redes internas.

En esta tarea de "conocer" han aparecido un gran número de libros, conferencias, eventos divulgando las técnicas de hacking en la búsqueda de mostrar cómo opera el enemigo.

En cada entrega de NEX IT Specialist, daremos bibliografía, pero aquí queremos destacar la serie de libros cuyos autores pertenecen a una de las empresas más prestigiosas de Seguridad Informatica (Foundstone Inc.: www.foundstone.com): www.hackingexposed.com. Casi todos han sido traducidos al español y editados en McGraw Hill/InterAmericana de España (lamentablemente las traducciones son paupérrimas!!!.Excepto el de "Hackers en Linux").

Instituciones privadas y gubernamentales también le han dado marco a toda una serie de actividades educativas y de divulgación. Destacamos el SANS Institute (www.sans.org), el ICS2 (www.ics2.com) creadora de la prestigiosa certificación CISSP, ver Págs. 40-41 en este ejemplar), The International Council of Electronic Commerce Consultants (EC-Council®) (http://www.eccouncil.org), The Institute for Security and Open Methodologies (ISECOM) www.isecom.org donde se definen estándares en test de seguridad y testeo de la integridad de los negocios.

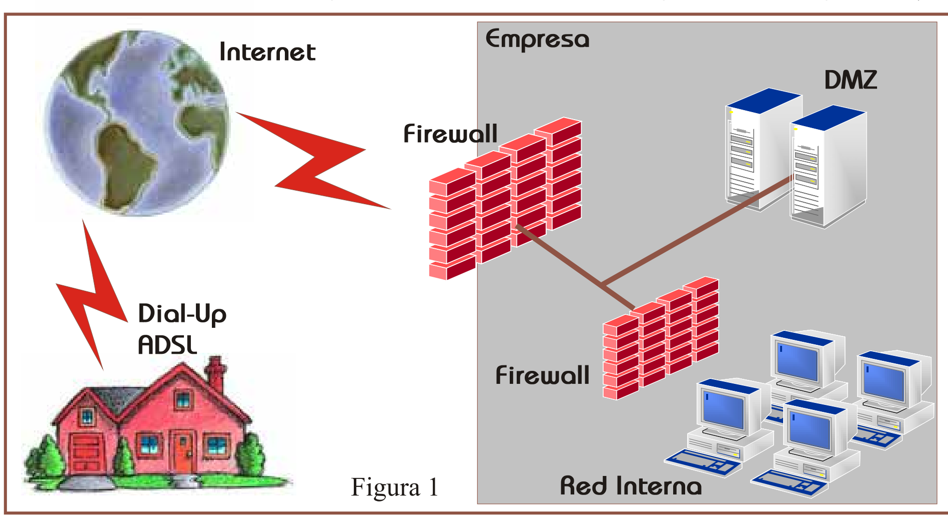


Figura 1



Cómo organizaremos entonces los artículos en esta serie?. Iremos exponiendo los temas imitando el modo en que actuaría un hacker. Iremos así abordando los siguientes tópicos en artículos sucesivos:

>> Footprinting
>> Scanning
>> Enumeration
>> System hacking (Windows, Linux, Unix, Novell (Netware).
>> Troyanos y backdoors (puertas traseras)
>> Sniffers
>> Denial of Service (DOS)
>> Ingeniería social
>> Hijacking de Sesión
>> Hackeo de servidores web
>> Cracking de passwords
>> SQL Injection
>> Hacking de redes wireless
>> Virus y Gusanos
>> IDS, Firewalls y Honeypots
>> Buffer Overfows
>> Metodologías de Tests de Penetración



Footprinting

(recolección de información)

La importancia del footprinting

Una de las acciones más importantes a la hora de hackear un sistema (o intentar) es obtener la máxima información disponible sobre él. En definitiva se trata de obtener las versiones de sus sistemas operativos, los puertos que tiene abiertos y toda información que nos pueda ser útil.
Cuando un ladrón se dirige a un Banco con intenciones de robarlo, él no solo camina al mostrador y dice "arriba las manos". Primero se toma su tiempo para recolectar la información necesaria para que su obra sea perfecta. Información sobre rutas de los autos blindados, los tiempos de entrega, cámaras de video, salidas de escape y un sinfín de detalles que lo ayudarán a cometer el delito con éxito.
Lo mismo sucede con los hackers cuando se plantean hackear un sistema, primero comienzan con lo que se llama "systematic footprinting", que simplemente es obtener información relevante como para crear un perfil de la configuración de seguridad de dicho sistema, organización, etc.

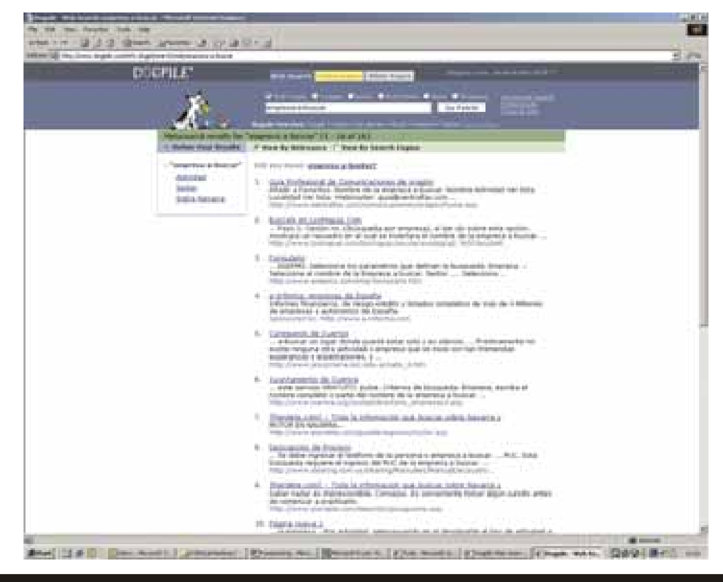
Como realizar el footprinting

Resulta difícil dar una guía para efectuar el footprinting (a veces llamado "actividades de rastreo"), ya que es una actividad que puede conducir a varios caminos posibles. Sin embargo, aquí esbozamos algunas acciones que le permitirán realizar dicho análisis.

¿Cómo procedemos?

El primer punto a resolver es determinar el ámbito de las actividades de rastreo. ¿Va a analizar la estructura de toda una empresa o bien va a limitar sus actividades a ciertas ubicaciones (por ejemplo, sedes o filiales)? En ciertos casos, la tarea de determinar todas las entidades asociadas a una empresa puede ser un tanto desalentadora. Internet pone a nuestra disposición una gran cantidad de recursos que podrá utilizar y que le ayudarán a reducir el ámbito de sus actividades, así como también ideas sobre el tipo y cantidad de información publica de una empresa y sus empleados.
Como punto de partida examine la página web de la empresa objetivo, si es que tiene una. Muchas veces una página web de una empresa proporciona una





cantidad increíble de información que puede ayudar a los atacantes. Se ha llegado a ver incluso las opciones de configuración de seguridad de sus firewall en los servidores web de Internet de algunas empresas. Otros puntos de interés son:

>> Ubicaciones
>> Compañías o entidades relacionadas
>> Noticias de fusiones o adquisiciones
>> Números de teléfono
>> Nombres de contacto y direcciones de correo electrónico
>> Directivas de seguridad o privacidad que indiquen los tipos de mecanismos de seguridad instalados
>> Enlaces a otros servidores web relacionados con la empresa

Ahora lo que debemos hacer es identificar nombres de dominio y redes asociadas relacionadas con la empresa en particular. Los nombres de dominio representan la presencia de la compañía en Internet y son, en Internet, el equivalente al nombre de su compañía, por ejemplo, "nombre-empresa.com.ar".

Existen numerosas bases de datos que podrá consultar y que proporcionan gran cantidad de información sobre las distintas entidades cuyo rastro esté intentando seguir. Hasta hace un tiempo, la compañía Network Solutions tuvo el monopolio como registro principal de los nombres de dominio: .com, .net, .edu y.org), pero en la actualidad existen numerosos registros disponibles.

Si disponemos de un sistema operativo tipo UNIX, podemos utilizar el comando "whois" o "xwhois". En Windows, podemos utilizar programas como "Netscan" o "Sam Spade". Estos programas o comandos nos muestran la información disponible sobre el dominio que le consultamos. Con esto logramos obtener información sobre:

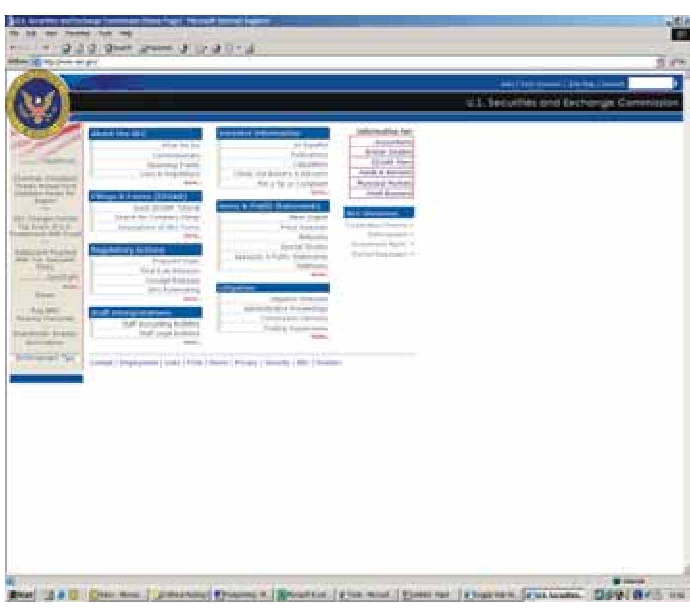
>> El nombre del administrador

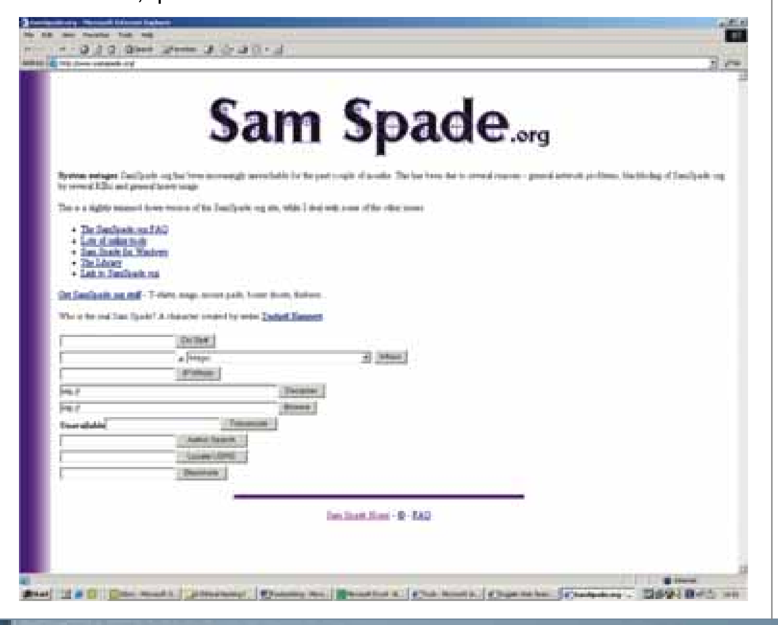
```
[bash]$ whois "empresa."@whois.crsnic.net
[whois.crsnic.net]Whois Server Versión 1.1

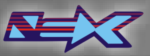
Domain Names in the .com, .net, and .org
domains can now be registered with many
different competing registrars. Go to
http://www.internic.net for detailed
information.

empresa-travel.com
empresa.net
empresa.org
empresas.com
```

Con el comando **whois***, si ponemos un "." al final del dominio a consultar, se listarán todos los dominios que comiencen con el nombre de la empresa.*









el registro
- >> Los servidores DNS primarios y secundarios
- >> Los dominios asociados al de la empresa.

Después de haber identificado todos los dominios asociados, podrá comenzar a consultar los DNS. El DNS es una base de datos distribuida que se utiliza para la transformar las direcciones IP en los nombres de host, y viceversa. Si un DNS está configurado de forma insegura, es posible obtener información muy relevante sobre la empresa. El comando "nslookup" es la herramienta más popular para realizar dicha tarea.

Ahora que ya hemos identificado las redes potenciales, podemos intentar determinar su topología, así como sus rutas de acceso potenciales.

Para esto, existe una herramienta llamada "traceroute" que nos permite seguir un paquete IP desde un host al siguiente. Es decir, analiza la ruta que sigue un paquete dentro de una determinada red, y así permite detectar redes activas, filtrador de paquetes o firewalls.

Si preferimos el entorno grafico, podemos utilizar el VisualRoute, que no solo nos proporciona información de las rutas, sino que también la localización geográfica.



Herramientas

Existen infinidad de herramientas en Internet que nos facilitarán información o nos ayudarán a encontrar lo que buscamos. En la siguiente tabla enumeramos alguna de ellas con sus respectivas páginas web.

Contramedidas

Hemos visto las técnicas y herramientas de footprinting. Existen muchas contramedidas. Por ejemplo muchos programas y herramientas comerciales permiten la detección de intrusos en la red (llamado Network Intrution Detection Systems) NIDS. Quizás uno de los mejores es gratuito: SNORT (www.snort.org) de Marty Roesch al cual dedicaremos uno de nuestros artículos de Paso a Paso. Humble de Rhino9 ha desarrollado un programa llamadoRotoRouter (http://packetstorm.security.com/UNIX/loggers/rr-1.0.tgz) . Este le permitirá registrar las solicitudes del *traceroute* generando respuestas falsas. Siempre podrá configurar sus routers frontera limitando el tráfico ICMP y UDP. ◀

Juan Manuel Zolezzi

```
[bash]$ nslookup
Default Server: dns2.acme.net
Address: 10.10.20.2

>> server 10.10.10.2

Default Server: [10.10.10.2]
Address: 10.10.10.2

>> set type=any
>> ls d Acme.net. >> /tmp/zone_out
```

ARIN database	http://www.arin.net/whois/
Cyberarmy	http://www.cyberarmy.com
Dogpile (meta search engine)	http://www.dogpile.com
DomTools (axfr)	http://www.domtools.com/pub/domtools1.4.0.tar.gz
Ferretsoft	http://www.ferretsoft.com
Sam Spade	http://www.samspade.org
Securities and Exchange Commission (SEC)	http://www.sec.gov/
USENET Searching	http://www.deja.com http://www.dogpile.com
VisualRoute	http://www.visualroute.com
WHOIS database	http://www.networksolutions.com
WS_ Ping Pack Pro	http://www.ipswitch.com




Wireless: el futuro

(Wi-Max, Mobile-Fi, ZigBee y Ultrawideband)

Aún hoy, existen localidades remotas que no pueden gozar de las tecnologías tradicionales de banda ancha para tener acceso a Internet. Causa fundamental: el costo.

Pero esto está por cambiar. Por ejemplo el gigante inglés de las telecomunicaciones British Telecom (BT) ha invitado a 100 usuarios de un pueblito en Irlanda del Norte y de otras áreas rurales interesados en la web a probar las nuevas y prometedoras tecnologías del futuro cercano. BT ha instalado una serie de torres de transmisión de radio que emiten señales por toda la región a pequeñas antenas a los costados de las casas de los clientes. La conexión será tan veloz como la banda ancha actual pero muchísimo más económica. ¿Por qué? Porque se utiliza equipo mucho menos costoso y un pedazo del espectro electromagnético (en la región de las ondas de radio) que no debe pagar licencias. De esta manera se evitan millones en pago de fees. Si el experimento resulta exitoso BT impondrá el año próximo este tipo de tecnología todo a lo largo y ancho de las Islas Británicas. "Esto revolucionará a la sociedad, del mismo modo que la telefonía móvil revolucionó a la sociedad en los años 80", dijo Mike Galvin, el director de Operaciones de Internet en BT.

¿Es esto todo? No, esto es sólo un ejemplo de cómo la porción sin licenciar del espectro de radio se está transformando en algo muy pero muy especial. Durante muchos años estas frecuencias de radio fueron tomadas sin interés, dejadas para los teléfonos inalámbricos de las casas y los aparatos de microondas. Pero en los últimos años ingenieros del MIT y Phillips han estado trabajando en tecnologías basadas en este pequeño ancho de banda del espectro de radio. Estos estudios han sido los que lograron implementar la tecnología WiFi que actualmente domina todo lo que sea conectividad de redes wireless.

Pero WiFi es sólo un pequeño escalón de las que serán 4 tecnologías innovadoras: Wi-Max, Mobile-Fi, ZigBee y Ultrawideband (Ultra Banda Ancha). Estas 4 tecnologías llevarán el networking inalámbrico a todas las facetas de nuestra vida diaria. Desde autos y hogares a edificios de oficinas y fabricas. Estas nuevas tecnologías ya han atraído en los últimos cinco años 4.500 millones de U$ en capitales de riesgo. Los productos basados en ellas estarán ya disponibles durante 2005. Harán que Internet se expanda creando la posibilidad de conectividad en cualquier parte y en cualquier momento. Se contará con herramientas que permitirán la resolución de todo tipo de problemas, ya sea conectividad dentro de un radio de unos pocos centímetros a kilómetros.

Una nueva era para la Web inalámbrica comienza. Estas tecnologías trabajarán entre sí y con las tradicionales tecnologías de la telefonía celular permitiendo que gente y máquinas puedan comunicarse entre sí. Pequeños pueblos podrán tener conexiones de red muy veloces. Viajando por autopistas podremos conectarnos usando laptops o PDAs para chequear el clima o cómo está el tráfico en la ruta. En los hogares podremos ver películas captándolas de antenas parabólicas con las computadoras transfiriéndolas a nuestras TVs con pantallas planas. Todo esto SIN CABLES. Y, pequeños sensores ubicados en rascacielos controlarán las luces, y hasta podrán hacer un monitoreo de los niveles de toxicidad del agua de los desagües. Llegará a lo que se llamara el "Internet de los objetos", donde máquinas inteligentes se comunicarán entre sí para decidir acciones que deberán tomar."

¿Cuáles son entonces estas tecnologías de futuro cercano? ZigBee por ejemplo, con su tecnología estándar de radio coordinará la comunicación entre miles de pequeños sensores. Estos sensores estarán distribuidos entre oficinas, granjas, o fábricas levantando información como temperatura, químicos, agua o aún movimiento. Estarán diseñados para consumir muy poca energía ya que



deberán permanecer en su lugar por diez años. Así, se comunicarán muy eficientemente pasando la información a través de las ondas de radio.

Al final del camino los datos podrán ser dejados en una computadora para ser analizados o levantados por otra tecnología como WiMax. Productos que utilicen ZigBee ya aparecerán en el mercado a fin de año.

Hot Spots Enormes

Wi-Max y WiFi son de algún modo similares. Para ambos se crean los llamados hot spots (puntos de acceso calientes) o áreas alrededor de una antena central donde la gente de forma inalámbrica puede compartir información o acceder a la Internet con una laptop apropiada. Mientras que WiFi puede cubrir unos 100 metros WIMax tiene un rango de 50 Km. Esto es, puede reemplazar las actuales conexiones de banda ancha que utilizan líneas telefónicas y cable. Es justamente una versión de prueba de Wi-Max la que usará BT en Irlanda. Wi-Max aún no puede ser usada si se está en movimiento (por ejemplo en un auto). Pero aquellos que están atrás de la tecnología (como Intel y Alcatel) planean tener una versión móvil en pocos años. Un estándar similar, Mobile-Fi estará disponible en 2 o 3 años. Esto permitirá conexiones más veloces que las actuales de banda ancha y realizados desde autos o trenes.

Finalmente Ultrawideband. Esta tecnología sirve otro propósito. Permitirá a la gente mover archivos enormes de modo muy rápido sobre distancias cortas. Esto permitirá llevar programas enteros en el hogar (por ejemplo de TV) desde la PC a la TV sin utilizar cables de ningún tipo.

En la ruta un conductor que reciba en su baúl, con su laptop, información usando Mobile-Fi podría usar Ultrawideband para llevar esa información a su computadora de mano en el asiento delantero. Aunque el estándar no está terminado Motorola ya esta vendiendo chips con esta tecnología.

¿Qué hace a estas tecnologías tan atractivas? Una es la naturaleza NO LICENCIADA de un pedazo de espectro de radio. Normalmente gigantes como AT&T pagan al gobierno enormes cantidades de dinero para poder operar en frecuencias de radio especiales.

Esto permitió poder proveerle a sus clientes telefonía celular sin interferencia, pero bloqueaba a otros de utilizar dicha frecuencia. Todas las nuevas tecnologías están basadas en el la parte del espectro NO LICENCIADA.

WiFi sentó el precedente de éxito que estas nuevas tecnologías intentarán imitar.

Un grupo de empresas se unieron para definir el estándar WiFi iniciando un círculo virtuoso. Altos volúmenes de venta bajaron los precios del equipamiento, los bajos costos abrieron la demanda y la gran demanda llevó a volúmenes de venta más grandes aún.

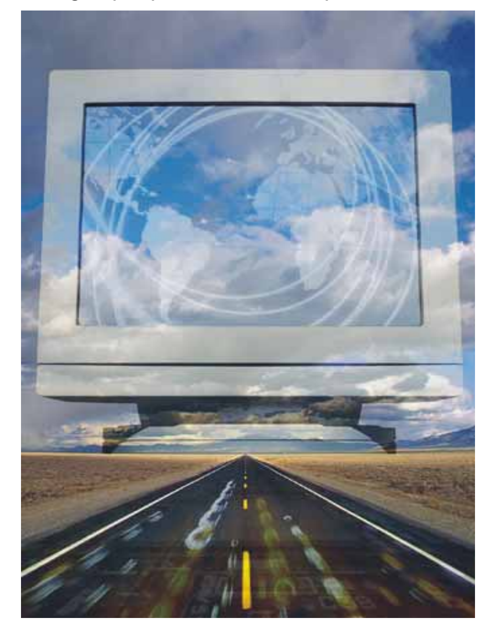
Ahora por ejemplo INTEL que comenzó el ciclo con unos 400 millones de dólares, vende chips Wi-Fi a fabricantes de computadoras por U$S 20 cada uno.



Un año antes se vendían a U$S 45. Unas 54 millones de laptops, PDAs y otros dispositivos Wi-Fi serán vendidos este año.

Todas estas tecnologías deberán vencer varios desafíos si desean imponerse. Los gigantes aún debaten sobre los estándares de Mobile-Fi y Ultrawideband y será recién en 2006 cuando quedarán definidos. Hasta entonces quienes fabriquen equipos no podrán comenzar producciones en masa lo que no permitirá baja de precios. Mobile-Fi está planeada para el espectro licenciado podría no triunfar si se logra agregar capacidades de movilidad a Wi-Max.

¿Y qué pasa con la competencia? Por



ejemplo las compañías de celulares están sacando una tecnología que les permitirá a sus clientes tener conexiones de RED en sus teléfonos móviles y laptops. Esta, llamada 3era generación, o 3G, competirá directamente con WiMax y Mobile-Fi. Ya hay empresas que han instalado esta tecnología en áreas de Washington y San Diego en USA, Europa y Asia. La tecnología 3G puede ser más lenta que Wi-Max pero es muy confiable y ya disponible.

Aún si WiMax y las otras logran triunfar hay otro desafío: una escasez de espectro de frecuencias. Todas ellas usando el mismo espectro podrían llegar a interferirse. Para evitar tal problema empresas como Intel, Microsoft y otras están haciendo lobby a la FCC (Federal Communications Comisión) para más espectro. ¿Su meta? Los grandes emisores de TV incluyendo ABC, NBC, y CBS que están sentados sobre grandes cantidades de espectro para transmitir programas de TV. La FCC ha estado promoviendo el uso del espectro sin licenciar pero no es claro que quiera entrar en conflicto con las grandes emisoras de TV.

Automatización

Una de las razones de optimismo es que estas tecnologías podrán ofrecer beneficios de modo de hacer un shock en la economía. Internet wireless promete elevar la productividad colectando información que no podía registrarse anteriormente y haciendo que esta información esté disponible cuando se la necesite. Esto acelera la automatización. Ejemplo: que un cajero haga tareas más productivas que solamente sentarse a registrar los productos de cliente. Ya Wi-Fi es usado por grandes tiendas de USA para inventarios y precios. Ahora la tecnología se esta moviendo a la construcción, servicios de rescate, salud y otros mercados. Se espera que combinadas estas tecnologías lleguen a 17.000 millones en ventas en 2007 de 3.300 millones del 2003. La próxima ola de productividad personal en el trabajo tiene que ver con movilidad. Las personas queriendo tener acceso desde cualquier parte.

Hay signos de mucho interés en estas tecnologías: Andover Controls Corp, que posee 100.000 sistemas de control de edificios instalados en el mundo, trabajó junto a Goodman Manufacturing Co para bajar el gasto energético en un 10% con sensores ZigBee.

En un test realizado se pusieron 4 sensores del tamaño de una caja de fósforos en cerca de 25 cuartos de hotel en Texas. Uno puesto en el aire acondicionado. Otros en las paredes para monitorear movimiento y temperatura en el cuarto.

Los sensores detectan si el aire acondicionado está prendido. Luego, una computadora central analiza la información y decide qué acción tomar.

Las aplicaciones de esta tecnologías pueden ser aún más ambiciosas. Por ejemplo, el departamento de energía de US ha contratado a Honeywell International Inc para usar sensores Zig-bee para ayudar a bajar costos de energía en un 15% en las industrias del acero, aluminio y otras seis. A modo de prueba, estos sensores se instalarán este año en empresas como Alcoa, ExxonMobil, para monitorear perdidas de energía de las cañerías y el uso de gases en los procesos de producción. Estos procesos usan grandes cantidades de calor y energía para transformar gases como hidrocarburos en etileno que se usa para fabricar plásticos. Los sensores de Honeywell harán un seguimiento continuo de la cantidad de gas utilizado. Esto será muy diferente a la evaluación que se hace una vez al día hoy. Esto permitirá a las compañías eliminar pérdidas o malgasto inmediatamente. Se estima que estas tecnologías wireless ayudarán a ahorrar 256 trillones de Btu de energía al año. Esto es más de la energía que utiliza una ciudad como Washington DC en un año.

Como las investigaciones continúan los sensores serán más pequeños y más versátiles. Eventualmente se espera llegarán a ser tan diminutos del tamaño de las partículas de polvo. Miles de estos pequeños sensores o “smart dust”

(polvo inteligente) podrían liberarse en la atmósfera para chequear cosas que van desde armas químicas a cambios climáticos.

Una vez que comiencen a integrarse, estas tecnologías permitirán otras innovaciones. Se espera que teléfonos celulares y laptops podrán cambiar el tipo de tecnología usada saltando de Wi-Fi a Wi-Max o la red tradicional telefónica. Por ejemplo los fabricantes de telefonía celular (Nokia, LG, Samsung) están incorporando tecnología Wi-Fi este año.

Se esperan entonces nuevos servicios. Por ejemplo un proveedor de electricidad podría ofrecer descuentos a aquellos que utilicen sensores Zig Bee para monitorear su uso de electricidad con precios diferentes dependiendo de la demanda.

Hoy, ya universidades y varias empresas envían sus llamadas telefónicas sobre Wi-Fi. Dartmouth College en USA tiene una red WiFi sobre su campus y



permite a los estudiantes hacer llamadas domesticas gratis usando sus laptops.

Ahora están probando video wireless con la idea de ofrecer programación de TV-por cable sobre Wi-Fi.

Este será pago para los estudiantes pero ahorrará, ya que no habrá que mantener tres diferentes redes: cable, teléfono y servicio de RED.

Después de su éxito con WiFi, Intel intentará lo mismo con Wi-Max. Un MODEM Wi-Max costará U$S 450 que es mas que los U$S 50 de un MODEM banda ancha o los U$S 200 de una tarjeta de telefonía 3G.

Pero se espera que Wi-Max dará velocidades de 5-10Mbits por segundo que es muchísimo mas que los 3Mbit por segundo de banda ancha o 300 a 5000 kilo bits por segundo de 3G.

Tanto Intel, Siemens, Alcatel, y Motorota han anunciado que incorporaran Wi-Max a sus productos y creen que van a lograr atraer mercado y lograr bajar los precios. Muchos parecen aun proyectos e ideas en desarrollo. Pero, eso es lo que flota en el ambiente y paso a paso se va concretando.

Novell y su compromiso con el Open Source.

La compra de Suse Linux y Ximian.

Entrevista con Alfred Mesguich, Regional Mananger para el Sur de

P:La compra de SuSE ha levantado un gran revuelo entre la comunidad open source. Sin embargo no se si estará de acuerdo conmigo en que no debería sorprender tanto que Novell apueste al mundo Linux tras algunos movimientos anteriores, como la compra de Ximian.

AM: No sólo por la compra de Ximian, sino también porque el compromiso de Novell con la comunidad de código abierto viene de largo. La estrategia multiplataforma de Novell se remonta a 1999, cuando se anunció que nuestro servicio de directorio, eDirectory, era capaz de trabajar con plataformas distintas a NetWare.
Desde entonces, y de forma continua, hemos ido añadiendo esta capacidad multiplataforma a otras muchas de nuestras soluciones. Asimismo, Novell lleva años participando en proyectos como Apache y Open LDAP, y también diseñó iniciativas como el sitio Novell Forge (http://forge.novell.com), desde el que se facilitaba el acceso a las iniciativas de fuente abierta de la compañía.
En abril del año pasado hicimos pública la intención de entregar todos nuestros servicios de red con los kernels tanto de Linux como de NetWare y ya en la última versión de NerWare se introdujeron características de código abierto, incluyendo MySQL, Apache y Tomcat, entre otras. El pasado mes de agosto adquirimos la compañía Ximian, mediante la que incorporamos a nuestra oferta distintas soluciones de gestión y de escritorio para Linux. Además, profesionales de reconocido prestigio internacional en el desarrollo de soluciones de fuente abierta como Miguel de Icaza y Nat Friedman se unieron a nuestro equipo.
Ahora, con SuSE LINUX, damos un importante paso en esta estrategia y en este mercado, mejora nuestra oferta, y se enriquece nuestro equipo de expertos en Linux y nuestros clientes consiguen una libertad total a la hora de elegir el sistema y la plataforma con la que quieren trabajar, consiguen gestionar y asegurar sus entornos y sus procesos de negocios con un costo inmejorable.
Linux, por tanto, es un mercado estratégico para Novell, y SuSE Linux y Ximian son líderes que gozan del mejor reconocimiento en este sector. La experiencia de las tres compañías y sus sólidas posiciones en el mercado les convierten en la mejor elección tanto para nuestros clientes como para nuestros partners.
Por otra parte, la comunidad de código abierto no tiene por qué preocuparse. Novell no quiere hacer a Linux propietario, todo lo contrario, Novell quiere potenciar el desarrollo del movimiento de fuente abierta. Creo que el respaldo de Novell puede resultar decisivo para que las compañías de esta comunidad consigan la masa crítica de negocio suficiente como para seguir creciendo.

P:¿Desde cuándo se estaba gestando esta compra en el interior de la compañía y que factores les hicieron decidirse por SuSE y no por otra empresa?

AM: Como he señalado en la pregunta anterior, el compromiso de Novell con la plataforma de código abierto viene de lejos y la compra de SuSE LINUX se llevó a cabo cuando todos los detalles de la estrategia de Novell en este sentido estuvo definida. La posición de SuSE LINUX en el mercado, su experiencia en Linux y su oferta de soluciones fueron los factores decisivos a la hora de decidirse por esta empresa.

P:Los rumores aseguran que la compra de SuSE se ha realizado para volver a recuperar la fuerza de Novell en el mercado de servidores, ya que NetWare no ha logrado los objetivos y RedHat parece que va ganando terreno. ¿Esto es cierto?.

AM: NetWare actualmente está implantado en miles de empresas líderes de todos los sectores empresariales del mundo, así como en organismos de la Administración, tales como British Telecom, Volvo, Lufthansa o en el Ministerio de Hacienda de Suecia. NetWare es muy importante en Novell y, aunque también hay que tener en cuenta que Novell es mucho más que NetWare, sin lugar a dudas nuestra orientación a Linux va a servir para incrementar la presencia de NetWare en el mercado.
También hay que aclarar que Novell ha desarrollado y mejorado NetWare, que Novell no va a abandonar NetWare, sino que va a añadir Linux para darles a nuestros clientes la libertad de elección de trabajar con la opción tecnológica que ellos decidan.

P:Y en esta línea, ¿tiene Novell los conocimientos necesarios para dar servicio, etc, en base al futuro desarrollo de SuSE dentro de la línea de negocio? Y, por cierto, ¿exactamente que peso tendrá la distribución SuSE en el negocio de la compañía?



AM: Novell cuenta con una organización global de servicios de consultoría, formación y soporte técnico, que supone uno de los principales valores añadidos en la oferta de nuestra compañía. Otros valores son su oferta de soluciones, que convierte a Novell en el único proveedor tecnológico capaz de presentar al mercado un conjunto completo de soluciones tecnológicas sobre Linux, tanto para los entornos servidor como escritorio, al que se unen las mejores herramientas de seguridad, networking, colaboración y gestión.
También hay que tener en cuenta al equipo humano que han incorporado Ximian y SuSE LINUX a la organización de Novell, un equipo del que forman parte los mejores expertos a nivel mundial del mundo Linux. Finalmente hay que recordar a nuestros partners, compañías altamente especializadas y con la capacidad suficiente para poder ofrecer al cliente el mejor servicio.
De esta forma podemos ofrecer a nuestros clientes la posibilidad de desplegar Linux en escenarios de misión crítica de una forma sencilla y con toda la confianza. Estableciendo una base sólida para que puedan establecer una estrategia a largo plazo en torno a la plataforma de código abierto y a los servicios basados en ella. En cuanto al negocio de SuSE Linux su facturación estuvo, durante el 2003 en torno a los 35-40 millones de dólares. Se espera que experimente un crecimiento en torno al 30 por ciento, que es el crecimiento.



medio que presenta la industria Linux. La facturación de Novell se sitúa en torno al los 1.000 millones de dólares.

P:¿Qué pasará con los últimos acuerdos que SuSE había realizado en estos meses? ¿Y cómo exactamente se están estipulando los acuerdos con IBM con Novell? Hay por ahí una inversión de 50 millones de dólares…

AM:IBM ha hecho pública su intención de invertir 50 millones de dólares en el capital de Novell, algo que supone un apoyo explícito a la estrategia de nuestra compañía. Pero no ha sido el único en mostrar públicamente su apoyo, otros como Dell o HP también lo han hecho.
Por otra parte SuSE mantenía otro acuerdo con IBM que afectaba el soporte SuSE LINUX para la plataforma eServer de IBM. Este acuerdo viene ahora a reforzarse y seguiremos trabajando para mejorar, si cabe, esta relación.

P:¿Cambiará la marca de SuSE, se creará una nueva compañía o…? ¿Cuál va a ser la estrategia seguir y que productos de Novell serán poco a poco sustituidos por los de SuSE?

AM: Con carácter general SuSE LINUX se convierte en una unidad de negocio Novell, de cuya dirección se harán cargo los departamentos comercial y de marketing de Novell de cada país, en los que, a su vez, se integrarán los equipos actuales de SuSE LINUX. Esta integración no va a afectar en ningún momento en la relación que mantienen SuSE LINUX y Novell con sus clientes, que seguirán recibiendo el soporte comercial y técnico al que estaban acostumbrados. No habrá en ningún momento interrupción de actividad.
La marca SuSE LINUX permanecerá y los productos de esta compañía se integrarán en la oferta de Novell. Quizá tengan que cambiar los nombres de determinados productos…de momento no se ha establecido el *roadmap* final de soluciones.

P:¿Qué mensaje quiere trasladar a la comunidad open source temerosa de cambios que les desfavorezcan tras la compra de SuSE? ¿Y qué mensaje a las empresas y sus clientes?

AM: Como he dicho anteriormente, Novell no quiere hacer a Linux propietario sino potenciar el desarrollo del movimiento de fuente abierta y conseguir incrementar el volumen de negocio que necesita para su progreso. A nuestros clientes, decirles que ahora, al trabajar con Novell, trabajarán con el único proveedor tecnológico capaz de presentarles una oferta de soluciones y servicios tan amplia a nivel global y el único en poder proporcionarles la libertad necesaria para que puedan decidir con toda libertad y con toda confianza la tecnología que quieren utilizar para hacer crecer su negocio.

Fuente Linux Free Magazine

SuSE y Ximian

SuSE Linux
www.suse.com

El 13 de enero de 2004, Novell finalizó la compra de SuSE LINUX, una combinación que ofrece a Linux soporte global técnico, servicios de consultoría y formación y redes y seguridad líderes en la industria, y que proporciona una alternativa atractiva para las compañías que deseen basarse en los numerosos beneficios del código abierto.

SuSE LINUX pasa a ser una unidad empresarial de producto dentro de Novell, y las ventas y marketing del producto serán gestionadas por las unidades empresariales geográficas de Novell, así como por el actual personal de marketing y ventas de SuSE LINUX. Novell mantendrá la marca SuSE LINUX, de gran fuerza en el mercado.

Ximian®,
www.ximian.com

Ximian es ahora parte de Novell. Es el proveedor más importante de soluciones desktop y server que ayudan a la adopción de Linux a nivel empresarial. Ximian ofrece un entorno completo de desktop y suite de productividad para Linux . También ofrece soluciones de administración de software a nivel empresarial de modo de dramáticamente reducir el costo de implementación y mantenimiento de sistemas Linux.

Los productos Ximian están en uso en todo el mundo por mas de 2000000 de personas y proveen la interoperabilidad, funcionalidad administrativa y facilidad de uso de modo de integrar los usuarios Linux y sistemas en entornos computacionales corporativos mixtos.Ximian tuvo su nacimiento en el proyecto GNOME. Este fue iniciado en 1997 por Miguel de Icaza, el co-fundador de Ximian y ahora Vice President of Product Technology para Novell. El esfuerzo atrajo rapidamente a un grupo talentoso de arquitectos e ingenieros. Estos incluyeron a Nat Friedman, cofundador de Ximinian y Vice President of Product Developmen para Novell.

El proyecto GNOME fue un rotundo éxito de los esfuerzo de la comunidad Open Source utilizando los esfuerzos de cientos de desarrolladores del mundo para producer una interface grafica para el usuario open source y aplicaciones de productividad para el desktop dentro del entorno UNIX, Linux y otros sistemas de codigo abierto.

En Octubre de 1999, de Icaza y Friedman fundaron Ximian (llamado entonces Helix Code) atrayendo cientos de arquitectos al proyecto GNOME, de modo de crear otros productos Open Source, servicios y herramientas de desarrollo basadas en GNOME.

Desde su nacimiento, Ximian ha logrado la adopcion de la plataforma linux y el desktop GNOME dentro de la industria. En Agosto del 2000, Ximian contribuya la creación de la fundación GNOME que hoy incluye a lideres de la industria como Sun Microsystems, IBM, Red Hat, HP, SuSE y otros. En Agosto 2003, Ximian fue adquirido por Novell, Inc. Transformándose en un componente fundamental de la estrategia Linux de Novell. Ahora, con el respaldo, y recursos de Novell, el grupo Ximian continúa cumpliendo un rol fundamental en la comunidad Open Source. Provee liderazgo y tecnologías basicas a proyectos importantes de la comunidad open source y grupos industriales, incluyendo GNOME, la Free Software Foundation y el recientemente anunciado proyecto Mono. Mono es una iniciativa de la comunidad para desarrollar una versión linux, open source, de la plataforma de desarrollo .NET de Microsoft.

Mono 1.0
www.go-mono.org

En Junio de 2004 Novell anunció Mono 1.0 una implementación open Source del framework .NET para ser usado en Linux, Unix y sistemas Windows. Mono consiste fundamentalmente de:

>> Un entorno avanzado de desarrollo para escribir aplicaciones Linux con una productividad sin precedentes.

>> APIs mejoradas para entregar aplicaciones cliente, servidor y servicios Web.

>> Capacidades de despliegue multiplataforma, soporte para Linux, Sun Solaris, Apple MacOS X, Microsoft Windows NT/XP y otros sistemas UNIX sobre una variedad de arquitecturas

>> Herramientas altamente efectivas que facilitan la creación de APIs y kits de desarrollo de software (SDK) que son lenguaje independiente a través de múltiples sistemas operativos.

>> Librería de programación multiplataforma Gtk# GUI que permite a los desarrolladores trabajar con Linux, Windows y MacOS X con un único código desde cualquiera de los lenguajes de programación de Mono.

>> Soporte para lenguajes tales como VisualBasic, Python, JScript y Java. A través del proyecto de fuente abierta iKVM, Mono incluye soporte Java, haciendo del popular lenguaje un vehículo capaz de respaldar la tecnología Mono.





Día nuevo, Novell nuevo



En un artículo bajo este título, realizado en eweek (www.eweek.com) sobre el evento anual de Novell de marzo 2004, "Brainshare", Steven J. V-Nichols nos comenta sobre el impacto que ha tenido dentro de la compañía sus movimientos hacia Linux.

El artículo es muy interesante ya que nos permite entender aún más la repercusión de las adquisiciones recientes de Ximian y SuSe. Nichols se pregunta fundamentalmente qué impacto tuvo dentro de Novell la nueva dirección tomada. Esto se vería respondido en Brainshare. Sabía que los ejecutivos estaban muy de acuerdo. ¿Pero, que pasaría con los partners de la vieja-escuela Novell, con los desarrolladores y los resellers?

La respuesta es que todos están encantados.

Por ejemplo, cuando Linus Torvals apareció brevemente uno de los días fue ovacionado por los presentes.

Comenta que por primera vez desde el lanzamiento de NetWare 4.0 en 1993, existe entusiasmo en el nuevo rumbo tomado por la empresa. Parte de este entusiasmo tiene que ver con que ven a Novell finalmente realizando un cambio profundo. Por muchos años Novell se ha movido lenta y muy cautelosamente en un mundo donde la competencia se mueve en forma muy ágil.

Llamó la atención de Nichols, que aún los desarrolladores participan activamente del entusiasmo. Hacer correr y administrar Novell es tan complicado como cualquier otro Sistema Operativo. Pero programar sobre Netware es complejo. Ser experto sobre las APIs (Application Programming Interface) de Netware y los Netware Loadable Modules (NLMS) es algo bastante difícil y exclusivo. Y, dejar de lado este expertise para comenzar a programar sobre Linux no es sencillo. Sin embargo nadie parece contrariado por el cambio.

Aún los resellers que son quienes deben enfrentar cara a cara a los clientes frente a un cambio muestran entusiasmo.

Interpreta Nichols que una de las rezones que contenta al mundo de los resellers es que Open Enterprise Server incluirá Netware y Linux. De este modo nadie se verá obligado a adoptar Linux compulsivamente.

La conclusión de Nichols: "Nace un nuevo día, un nuevo amanecer para Novell. Y, no solo lo dice Novell sino la gente que lo mantiene, aquellos que hacen sus negocios alrededor de Novell y que están disfrutando ver retornar una luz y vida a una vieja empresa"

¿Es conveniente certificarse en Linux?

Mucha gente está muy capacitada en Linux, pero muy pocos tienen certificaciones internacionales. Por ejemplo, hasta mediados del 2003 había solo 4 personas en Argentina certificados en LPI (Linux Professional Institute) nivel 2. La primera pregunta es si vale la pena certificarse en Linux. La respuesta es sí, ya que aquél que realiza el esfuerzo (tanto de aprendizaje como económico) mostrará a un futuro empleador su decisión de educarse y búsqueda de logros. Lamentablemente los costos (U$S 100.- por examen para LPI y varios cientos U$S en el caso Red Hat) son muy altos para el mercado argentino con relación a los salarios actuales.

La segunda pregunta es a qué certificación apunto. Existen cinco:

>CompTIA Linux+
>Red Hat (RHCE, Red Hat Certified Engineer, RHCT (Technician), RHCA (Architect).
>LPI (LPIC, Linux Professional Institute Certification),
>Novell, CLP (Certified Linux Professional) y CLE (Certified Linux Engineer)
>Sair Linux-LPC (una certificación poco popular)

En la Argentina las más populares son LPI y Red Hat. La certificación Novell es muy reciente (recordar que Novell adquirió a Ximian y Suse hace relativamente poco). LPIC es posible rendirla utilizando empresas como VUE (Virtual University Enterprise, www.vue.com) y Prometric (www.prometric.com). Red Hat debe realizarse en Red Hat mismo. En Argentina, Preteco SA (www.preteco.com) viene realizando promociones de cursos y exámenes a precios promocionales y los exámenes son rendidos en Argentina.

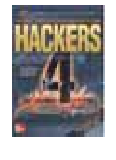




BooKs BooKs BooKs BooKs

Hackers 4

McClure Stuart, Joel Scambray, George Kurtz



El compendio definitivo de herramientas y prácticas de hacking. El mundo digital avanza rápidamente. Cada día aparecen nuevas herramientas, técnicas y metodologías que utilizan los hackers para introducirse en todo tipo de sistemas y redes. El best-seller "Hackers" se actualiza una vez más para tratar las últimas tecnologías y técnicas en el apasionante mundo de la seguridad.Esta nueva edición incluye un capitulo nuevo sobres los ultimos ataques y contramedidas de seguridad para redes inalámbricas, nuevas estrategias para defenderse de manera proactiva contra los ataques telefonicos, capitulo de hacking de sitios web, completamente revisado y actualizado para tratar las ultimas vulnerabilidades especificas de cada plataforma, desde Apache a IIS, y muchas otras cosas más.

CISSP All-in-one Exam Guide (segunda edición)

Shon Harris



Completa cobertura de todo el material necesario para rendir el examen CISSP (*Certified Information Systems Security Professional*). Esta edición actualizada con las últimas novedades, incluye los objetivos del examen, consejos, preguntas prácticas, fotografías e ilustraciones. También incluye un CD que contiene un examen simulado con más de 850 preguntas y respuestas y un video sobre criptografía. Indispensable no solo para aquellos interesados en el CISSP, sino también como biblioteca de consulta para todo administrador.



News (!)
Congreso de software libre
Breves (!)
Together Edition para Visual Studio.NET
Oracle y Microsoft se asocian
Sistema Dinámico de Archivos
COBOL - Comunidad virtual

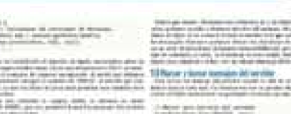


mobile



[white paper]
Programación orientada a aspectos
Crosscutting concerns en OOP







Java Mail
Cómo funciona



Nuestro primer contacto con Windows Firewall

La protección de la información en nuestra infraestructura computacional y la seguridad en las comunicaciones informáticas ha hecho primordial poder garantizarlas. Dentro de muchas acciones tomadas,

A partir de la salida próxima del SP2, se activará en XP automáticamente para todas las NICs el Windows Firewall (WF)l (anteriormente Internet Connection Firewall - ICF).

Esta decisión de Microsoft es muy importante ya que puede hacer funcionar a Windows XP de un modo diferente a lo que los usuarios están acostumbrados, ya sea que se esté trabajando en un dominio (es decir utilizando Active Directory) o en un grupo de trabajo. Puede causar, que cosas que antes funcionaban, dejen de hacerlo.

Muy probablemente terminaremos por configurar sus bloqueos de una manera no tan restrictiva, ya que por defecto WF deshabilita tanto el control como las herramientas de soporte remotas (recordar que éstas han sido las características distintivas de Windows XP). UD. deberá decidir si desea habitar o deshabilitar el WF en sus máquinas clientes. Y, quizás modificar los seteos que vienen por defecto. Lo que describimos a continuación es cómo hacer esto y cómo poder hacerlo fácilmente para muchísimas máquinas en la red que usted administra.

Windows Firewall: ¿qué es?, ¿para qué sirve?

Muchos se preguntarán qué hace exactamente Windows Firewall, o en realidad que va a hacer una vez implementado el SP2. Una buena respuesta sería: "examina y potencialmente bloquea el tráfico de entrada de paquetes de información. No afecta el tráfico de salida"

En su instalación por default, Windows Firewall rechazará todo el tráfico de entrada, a menos que el mismo sea en respuesta a un requerimiento previo de salida del sistema que lo tenga instalado. Por ejemplo si abrimos el explorador de Internet (IE) de una máquina con XP con SP2 instalados y escribimos *www.cortech.com.ar* en la barra de exploración, IE causa que el sistema envíe un requerimiento a COR por su página de inicio. Si bien Windows Firewall no bloquea el tráfico de salida, toma nota hacia donde se dirigen los paquetes. Entonces una vez que el Web Server de COR trata de enviar al IE la información que solicitó previamente, Windows Firewall detectará que ese tráfico que quiere ingresar proviene de *www.cortech.com.ar*, un sitio al cual el sistema había enviado un requerimiento, y lo deja pasar.

Esta forma de actuar de Windows Firewall garantizará que el sistema se pueda comunicar con el resto de Internet y con la intranet, pero solamente cuando sea el propio sistema el que inicia la conversación con los demás equipos.

La verdadera utilidad de este producto radica cuando un sistema externo trata de establecer una conversación con un sistema con XP y SP2 instalados y envía paquetes. Como Windows Firewall no interpreta la comunicación como una respuesta a un requerimiento previo de nuestro sistema, el firewall descarta cualquier paquete que quiera ingresar. Esto es de vital importancia cuando se trata de evitar el ingreso de virus y gusanos.

Pero, ¿qué pasaría al habilitar el Windows Firewall en un sistema dentro de una intranet conectada a un dominio? Podríamos pensar en un primer momento que todas las comunicaciones serían rechazadas excepto aquellas iniciadas por el propio sistema. Sin embargo analizando detenidamente la situación nos damos cuenta que toda comunicación dentro de un dominio es siempre iniciada por un cliente: el cliente pide para loguearse, el cliente pide para refrescar las group policies, el cliente pide por los perfiles remotos, etc.

La única funcionalidad que se perderá al activar Windows Firewall sin modificar su configuración inicial, es la de poder utilizar las herramientas de administración remota que vienen con Windows XP.

Habilitando y deshabilitando Windows Firewall

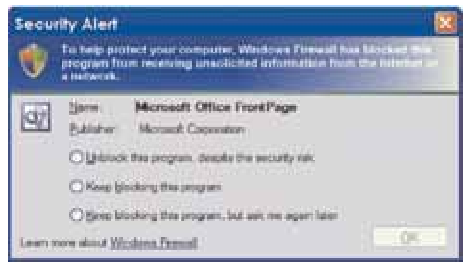
El aspecto de mayor relevancia, por lo menos inicialmente, para el control de Windows Firewall, es que el mismo podrá ser habilitado o deshabilitado bajo SP2 de tres maneras: a través de la interfase gráfica (GUI), desde la línea de comando, o a través de una group policy.

La GUI de Windows XP cambiará a partir de la salida de SP2. Por este motivo explicaremos brevemente como habilitar/deshabilitar Windows Firewall a través de este medio.

GUI y línea de comando

Dependiendo de cómo esté configurada la interfase, cuando se haga click en Inicio, Panel de Control, se debería ver una categoría llamada Conexiones de Red o también Conexiones de Red y Acceso a Internet.

Si lo que se ve es la primera opción, sobre el panel izquierdo verá la sección Tareas de Red que contiene un link de Configuración de Firewall de Conexión a Internet. Si en cambio se ve un link de Conexión LAN o Conexión Wireless, hay que hacer un click derecho sobre el mismo,





elegir Propiedades, Avanzadas y por último Configuración.

Si lo que se ve es la categoría Conexiones de Red y Acceso a Internet, deberíamos hacer click en esa categoría directamente, ahorrando unos cuantos pasos, y luego dentro de Elegir Tarea en el panel izquierdo, seleccionar la opción Configurar el Firewall.

De cualquiera de las dos formas antes mencionadas se llegará hasta una página de Propiedades del Firewall de Conexión a Internet. Dentro de esta página en la tabla llamada General, se ofrecen las tres opciones posibles: On, On sin excepciones, y Off.

Sin embargo, el usuario puede preferir modificar Windows Firewall por medio de la línea de comando, ya sea porque le es más cómodo o porque necesita cambiar la configuración en múltiples maquinas y no puede utilizar las group policies.

A partir de SP2 el ya existente comando Netsh adquirirá nuevas opciones para configurar Windows Firewall. Por ejemplo se puede apagar Windows Firewall en todos los sistemas abriendo un prompt de comando y escribiendo:

```
netsh firewall ipv4 set opmode
        mode = disable
```

Pero supongamos que no se quiere apagar Windows Firewall en todas las NICs, sino solamente habilitarlo para las NICs Wireless y deshabilitarlo

para las NICs Ethernet. Se puede usar el comando que vimos anteriormente pero con un agregado, el nombre de la interfase a la que le hacemos las modificaciones:

```
netsh firewall ipv4 set opmode
                    mode = enable
          interface = "wireless network
connection"
netsh firewall ipv4 set opmode
                    mode = disable
          interface = "local area connection"
```

Usando Group Policy para la configuración

El Service Pack 2 de Windows XP le dará la posibilidad al usuario de deshabilitar Windows Firewall desde el editor de Group Policy (GPE), ya sea como una política local o de dominio. SP2 traerá una nueva categoría de objetos de Group Policy (GPO) para controlar Windows Firewall.

Dentro del GPE se deberá navegar con el browser hasta Configuración de Computadora, Plantillas Administrativas, Grupo de Trabajo, Conexiones del Grupo de Trabajo, Firewall de Conexión a Internet, y dentro de esta última carpeta, encontraremos dos carpetas más: Perfil de Dominio y Perfil Móvil.

Dos perfiles posibles

Microsoft al momento de desarrollar el SP2 consideró que muchas personas no desearán tener habilitado Windows Firewall cuando se encuentren trabajando en red, pero sí necesitarán tenerlo habilitado cuando trabajen fuera de esa red. En consecuencia la empresa hizo al firewall lo suficientemente inteligente para determinar si el sistema donde está funcionando se encuentra o no, conectado dentro de un dominio. Entonces, cuando lo esté, Windows Firewall seguirá las instrucciones que figuren dentro de la carpeta de Perfil de Dominio antes mencionado. En cambio cuando detecte que el sistema no está conectado a un dominio, buscará dentro de la carpeta Perfil Móvil para seguir las instrucciones que allí se encuentren.

Cada una de estas carpetas tendrá las mismas nueve configuraciones de políticas, una de las cuales se llamará Modo de Operación, mediante la cual podrá deshabilitarse Windows Firewall.

El Modo de Operación tendrá otros dos estados posibles: habilitado y protegido (shielded). Este último estado hace que el firewall ignore todas las peticiones de los puertos abiertos. De esta forma, no se permitirá la entrada no solicitada de datos y se podría utilizar en caso de infección de gusanos para impedir la proliferación del virus dentro de la red.

Utilizar la línea de comando para configurar los perfiles

Para manejar el comportamiento de Windows Firewall dentro de un perfil en particular, solamente haría falta agregar el parámetro "perfil = " al comando de Netsh para configurar el modo de operación, seguido por la palabra actual, corporativo, todos, u otro. Actual indicará al sistema que realice el cambio en el perfil que se encuentra en ese momento activo. Todos, significa que el cambio se realizará para ambos perfiles. Corporativo y otro se utilizarán para realizar cambios, en el perfil de dominio el primero y en el perfil móvil el segundo.

Como ejemplo se puede mostrar una línea de comando que permitirá configurar el Windows Firewall como deshabilitado cuando el sistema se encuentre conectado a un dominio y habilitado en cualquier otro caso.

```
netsh firewall ipv4 set opmode
                    mode = disable
          profile = corporate
netsh firewall ipv4 set opmode
                    mode = enable
          profile = other
```

Configuraciones avanzadas

Si bien sólo hemos mencionado hasta el momento las características superficiales que traerá este producto, a partir de la salida del SP2 de Windows XP, con lo expuesto el usuario se encontrará en condiciones de configurar inicialmente Windows Firewall para trabajar



normalmente.

Queda pendiente quizás para una próxima edición investigar con mayor profundidad las bondades de este nuevo producto de Microsoft.

Rodrigo M. Gonzalez







NAT: Network Address Translation

Cada vez son menos las direcciones disponibles para que una computadora pueda conectarse a Internet. Producto de este agotamiento se han ido desarrollando diferentes métodos para solventar este problema.

Necesidades de su creación

En los últimos años, el crecimiento de Internet ha sido de una magnitud inimaginable superando ampliamente las expectativas para la época en que surgió.

Como sabemos, para conectarnos a Internet necesitamos que se nos otorgue un número de identificación única conocido como dirección IP el cual le sirve a una computadora para ser identificada en la red de forma única, en cualquier lugar del mundo y poder comunicarse con las demás. El mismo consta de 32 bits que, en su forma decimal, lo encontramos separados en cuatro grupos de 8 bits cada uno bajo la forma 168.200.34.2. En principio, con estos 32 bits estaríamos en condiciones de obtener 2^32 direcciones teóricamente posibles, o sea casi 4.300 millones de direcciones IP únicas. De esa cantidad debemos descartar aquellas direcciones que tienen fines específicos o que son utilizadas para determinados sectores no públicos. Esta forma de direccionamiento es conocida como IP versión 4 (IPv4).

A principios de los años ´90, cuando comenzó a gestarse Internet como la conocemos ahora, se creyó que esa cantidad era virtualmente inagotable. La explosión de Internet en los últimos años y el incremento de las redes hogareñas y comerciales han revertido esta situación, dado que son cada vez más los usuarios conectados en el mundo. La solución es implementar un sistema que permita obtener una mayor cantidad de direcciones. Hace años se está gestando una nueva forma de direccionamiento conocida como **IP versión 6** (IPv6), la cuál constaría de 128 bits, pero implementarla de manera eficaz llevaría a modificar toda la infraestructura de Internet.

Existe una solución de compromiso utilizando la infraestructura existente utilizando IPv4. Allí es donde entra en juego el servicio conocido como **NAT**.

NAT

Desarrollado por Cisco Systems Inc. para cubrir los requerimientos de direcciones IP insuficientes nace, bajo la recomendación RFC 1631, **N**etwork **A**ddress **T**ranslation o Traducción de Direcciones de Red. La idea es poder implementar un sistema mediante el cual un sólo dispositivo, tal como un router, actúe como agente mediador entre la red pública (Internet) y la red local privada (Intranet). Esto significa que una única dirección IP basta para representar a un grupo entero de computadoras con acceso a la red pública.

El servicio de traducción de direcciones funciona de manera similar a una secretaria recepcionista en una empresa. Digamos que Ud. le dio expresas órdenes a la recepcionista de no derivarle ninguna llamada telefónica a menos que Ud. así lo requiera. Supongamos que Ud. llama a un cliente potencial y le deja dicho que lo llame a su despacho. Ud. le comunica a su secretaria que espera un llamado de tal cliente y le indica que se lo derive a su despacho cuando éste llame. La secretaria toma apunte de tal pedido.

Acto seguido, el cliente llama al número principal de la empresa, que es el único que conoce. Éste pide hablar con Ud. La recepcionista chequea en su registro que coincida el nombre del cliente que debería llamar con la extensión (interno) que le corresponde a Ud., de acuerdo a las instrucciones que Ud. le impartió. Debido a esto, la recepcionista sabe que Ud. requirió tal llamada y se la deriva a su oficina.

La traducción de direcciones de red es utilizada por un dispositivo (firewall, router o computadora) que se sitúa entre la red interna y el resto del mundo.

Las direcciones IP sufren una clasificación en *direcciones públicas* y *direcciones privadas* . Las direcciones públicas son aquellas que un proveedor le asigna a un dispositivo para poder comunicarse con otro en Internet. Estas direcciones son administradas por un organismo internacional, el **IANA** (***I****nternet* ***A****ssigned* ***N****etwork* ***A****uthority*).

Las direcciones privadas son aquellas que pueden ser utilizadas en una red interna para direccionar a sus dispositivos. Estas direcciones pueden repetirse en diferentes redes locales por lo que son consideradas *no ruteables* ya que no pueden ser utilizadas en la red pública. Estas direcciones también se conocen como *no registradas*.

El IANA define bajo la RFC 1918, el rango de direcciones públicas y privadas. Ninguna compañía puede utilizar las direcciones privadas en la red pública. Además, los routers fueron diseñados para descartar los paquetes provenientes directamente de direcciones privadas.

Los rangos para direcciones privadas son los siguientes:

Rango 1: Clase A - 10.0.0.0 a 10.255.255.255
Rango 2: Clase B - 172.16.0.0 a 172.31.255.255
Rango 3: Clase C - 192.168.0.0 a 192.168.255.255

La red interna es usualmente una LAN (Local Area Network) a la que comúnmente se denomina **dominio stub** (no existe una traducción literal del vocablo *stub*, aunque el término más apropiado es el de *fragmento*). Un *dominio stub* es una LAN que utiliza direcciones IP internamente. La mayoría del tráfico de red en un *dominio stub* es local, es decir no traspasa la frontera de la red interna. Por este motivo, un *dominio stub* puede utilizar indistintamente direcciones registradas (públicas) o no registradas (privadas). De manera obvia, cualquier computadora que utilice direccionamiento privado deberá utilizar el servicio de traducción de direcciones de red para comunicarse con el resto del mundo.

NAT puede operar básicamente de varias maneras. Veamos tres:

- NAT dinámica
- NAT estática
- Sobrecarga de NAT

NAT Dinámica

Para configurar NAT en forma dinámica debemos contar con un rango de direcciones IP públicas otorgadas por el proveedor de servicios de Internet (ISP, Internet Service Provider). A este rango lo llamaremos pool de direcciones.La mayoría de las computadoras de la red interna se comunican con otras de la misma red utilizando direcciones locales

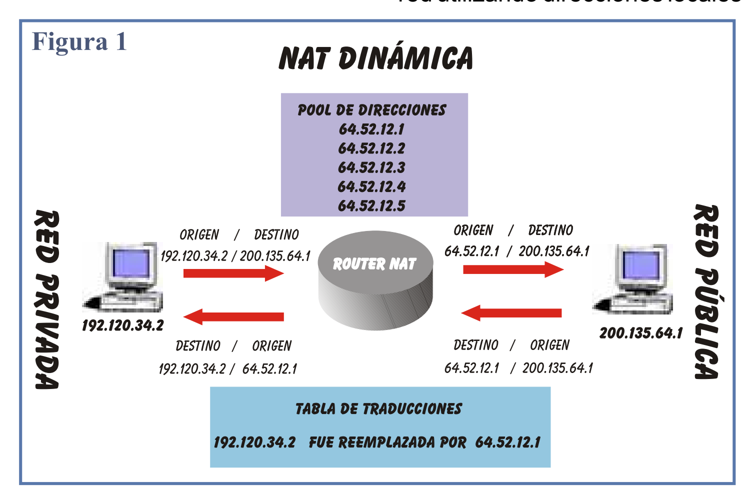


Figura 1



internas.

Aquellas computadoras que necesiten comunicarse con la red exterior y no tengan una dirección pública, enviarán los paquetes a través del router NAT. El router tomará el paquete y leerá las direcciones origen y destino para saber qué computadora emitió el paquete y cuál es el destino del mismo (192.120.34.2 / 200.135.64.1). Registrará en su tabla de traducciones la dirección origen (quién emitió) y la reemplazará por una dirección disponible del pool de direcciones que nos otorgó nuestro ISP (192.120.34.2 64.52.12.1). Luego enviará el paquete al destino pero con la dirección del pool haciéndole creer a la computadora destino que quién emitió el paquete tiene una dirección pública (64.52.12.1 / 200.135.64.1). Si en ese momento otra computadora deseara comunicarse con la red exterior, el router le asignaría la próxima dirección pública disponible del pool. Todo esto llevando un minucioso registro de cada reemplazo. **Ver Figura 1**.

Cuando la computadora de la red externa devuelve el paquete, éste es entregado a la dirección que la computadora creyó tener como origen real, o sea la dirección que el router tomó del pool (64.52.12.1). El router verificará en su tabla a quién le correspondía todo mensaje que entrase con dicha dirección 64.52.12.1. En su tabla tiene apuntado que corresponde a 192.120.34.2, quién verdaderamente emitió el paquete.

Con NAT dinámica, a la primera computadora que desea ingresar a la red pública, el router le asigna la primera dirección del pool, a la segunda computadora, la segunda dirección y así sucesivamente. Cuando la computadora en cuestión, ya no transmita más hacia la red exterior, la dirección del pool queda liberada para que el router pueda asignársela a otra computadora.

El router puede mantener tantas traducciones simultáneas como memoria DRAM posea. Una entrada en la tabla de enrutamiento ocupa algo así como 160 bytes, por lo tanto un router con 4MB de DRAM podrá alojar alrededor de 26.000 traducciones en forma simultánea, algo más que suficiente para la mayoría de las aplicaciones.

NAT Estática

El funcionamiento de NAT estática es exactamente igual que el anterior, salvo que en lugar de contar con un pool de varias direcciones públicas, contamos con una única dirección otorgada por el ISP. De esta manera sólo una computadora por vez puede salir al exterior ya que contamos con una única dirección. Cuando ésta deje de transmitir, quedará liberada la dirección para ser utilizada por otra computadora.

Debido a esto, generalmente se utiliza NAT estática para darle acceso exterior a un Web server por ejemplo, ya que se tratará siempre de la misma computadora la que se conecte al exterior.

Generalmente los ISP proveerán a una empresa de una única dirección IP, no de un pool de direcciones. Esto se debe a la escasez de direcciones y al alto costo de cada una de ellas debido a dicha escasez.

Si esto es así, cabe la pregunta ¿ cómo haremos para tener más de una computadora en nuestra red local y que cada una de ellas pueda ser direccionada a Internet con una única dirección pública asignada por nuestro ISP ? La respuesta es que el modo en que opera NAT estática no permite hacerlo. Esto ha dado que se origine una nueva forma de traducción de direcciones de red, denominada **sobrecarga de NAT** o **PAT**.

Sobrecarga de NAT PAT

Este método consiste en que varias direcciones privadas puedan ser direccionadas a Internet mediante una única dirección pública y el uso de diferentes puertos. Por esta razón el método es conocido como traducción de direcciones de puertos o **PAT** (***P****ort* ***A****ddress* ***T****ranslation*). Para realizar la sobrecarga de NAT, se utiliza una particularidad de la pila de protocolos TCP/IP conocida como **multiplexing** (multiplexado), la cual permite a una computadora mantener varias conexiones concurrentes con uno o más dispositivos remotos utilizando diferentes puertos TCP o UDP.

Recordemos que un paquete IP posee un encabezado que contiene la siguiente información:

Dirección origen (source address) : es la dirección IP del dispositivo que origina el paquete de datos, tal como 185.120.34.2.

Puerto origen (source port) : es el número de puerto TCP o UDP asignado por el dispositivo que origina la comunicación para enviar tal paquete. Ejemplo: puerto 1080.

Dirección destino (destination address) : es la dirección IP del dispositivo receptor del paquete, hacia quién va dirigido el mismo, tal como 200.135.64.1.

Puerto destino (destination port) : es el número de puerto TCP o UDP que el dispositivo origen le solicita que abra al dispositivo destino para que pueda recibir el paquete enviado. Ejemplo: puerto 3021.

Las direcciones IP definen a los dos dispositivos en cada extremo, mientras que los números de puertos aseguran que la conexión entre ellos tenga un identificador único. La combinación de estos cuatro parámetros define una conexión TCP/IP única. Cada número de puerto está definido por 16 bits, lo cual significa que la cantidad de puertos posibles son 65.536 (2^16).

En este ejemplo hemos representado por simplicidad la comunicación de una única computadora, a merced de que la técnica de PAT es evidente cuando transmiten simultáneamente más de una computadora. **Ver Figura 2**

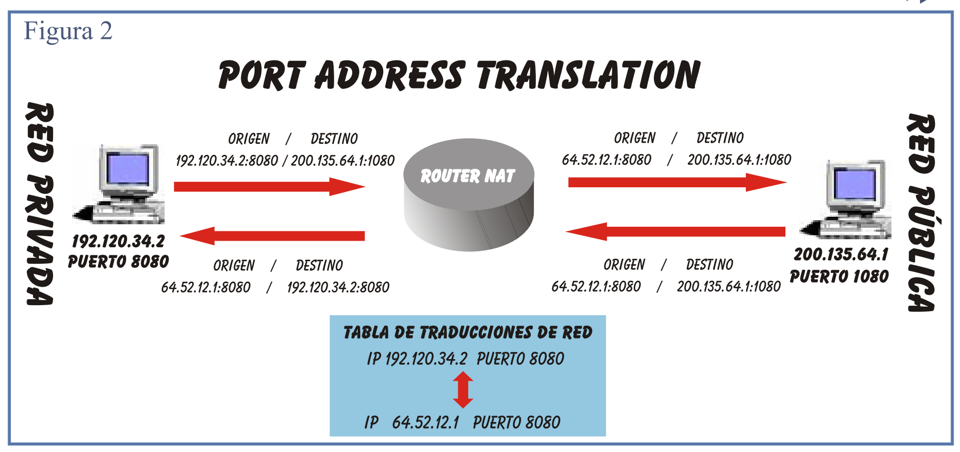
La computadora origen, cuya dirección IP es 192.120.34.2 utiliza el puerto 8080 para canalizar sus paquetes. El router registra en su tabla de direcciones, la dirección privada y el puerto de dicha computadora y procede a reemplazar esta dirección por la dirección IP pública asignada por el proveedor de Internet (64.52.12.1). Asimismo registra el puerto por el cual se originó el paquete (8080). Como el paquete enviado contiene la dirección y el puerto destino, éste alcanzará a la computadora en cuestión (200.135.64.1), puerto 1080.

Cuando ésta le regresa un paquete, utilizará como dirección destino la IP pública 64.52.12.1, puerto 8080, creyendo que desde ésta dirección es desde donde se originó el paquete. Cuando el router NAT recibe dicho paquete, lee su cabecera y detecta como destino el par 64.52.12.1:8080, combinación que, según su registro, pertenece a la IP 192.120.34.2 puerto 8080. Cambia la dirección con la que le llega por ésta última y procede a enviárselo a la computadora que originariamente generó la comunicación.

Si otra computadora deseara comunicarse con otra de la red pública antes de que termine la transmisión anterior, podrá hacerlo utilizando la misma IP pública 64.52.12.1, *pero utilizando un puerto diferente al ya citado 8080*.

Cada vez que el router registra un evento en su tabla de traducciones, se inicializa un temporizador con el objeto de controlar que no se acumulen entradas inútilmente. Si una entrada no es accedida antes de que el tiempo expire, ésta es retirada de la tabla de traducciones suponiendo que no se

Figura 2



volverá a utilizar, incrementando el espacio disponible para otros eventos.

Seguridad de NAT

Existen otras cualidades que nos ofrece NAT además de salvarnos de la escasez de direcciones IP. ¡ SEGURIDAD !

Implementando NAT dinámica se crea automáticamente un servicio de firewall entre la red interna e Internet. NAT permite únicamente conexiones que se originen en el interior del dominio stub. Esencialmente, significa que una computadora que se encuentre en la red externa no puede conectarse a una computadora de la red interna a menos que ésta haya iniciado la conexión. Uno puede navegar por Internet, conectarse a un sitio e incluso descargar un archivo, pero nadie del otro lado puede unirse a nuestra computadora a menos que lo permitamos.

NAT estática, por su parte, habilita a los dispositivos externos a iniciar conexiones hacia el dominio stub. Por ejemplo si deseamos conectarnos a una dirección IP interior asignada a un servidor Web, NAT debería habilitar esta conexión.

Algunos routers NAT proveen de filtrado y registro de tráfico. El filtrado permite controlar qué tipo de sitios son visitados en la Web y el registro de tráfico permite generar reportes de los mismos.

Muchas veces confundimos NAT con los servidores proxy, pero existen claras diferencias entre ellos. NAT es un servicio que resulta transparente tanto para los dispositivos origen como para los destino. Uno no percibe que se trata de una transacción con un tercer dispositivo, el router NAT. En cambio un servidor proxy no es transparente ya que la computadora origen "sabe" que se encuentra realizando una petición al servidor proxy y debe ser configurada para que realice esto. La computadora destino "piensa" que el servidor proxy es quién funciona como origen y trata con él directamente. Otra diferencia es que los servidores proxy trabajan normalmente en la capa de transporte o superior (capa 4) del modelo de referencia OSI, mientras que NAT es un servicio de direccionamiento de capa 3.

El hecho de trabajar en capas superiores hace que los servidores proxy sean, en la mayoría de los casos, más lentos en procesar información que los dispositivos que operan NAT.

En cuanto a lo que administración respecta, NAT posee cierto beneficio. Por ejemplo, podemos mudar el servidor Web o el servidor FTP a otra computadora host sin tener que preocuparnos por enlaces incompletos. Simplemente cambiando la configuración interna en el router para reflejar al nuevo host. Podemos hacer cambios a la red interna fácilmente a causa de que la dirección IP externa o pertenece al router o proviene de un pool de direcciones. NAT y DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) son una combinación justa.

Podemos elegir un rango de direcciones privadas para nuestro dominio stub y dejar que el servidor DHCP se encargue de acomodarlas como sea necesario. Esto hace mucho más fácil la escalabilidad de la red. Al no requerir más direcciones públicas que la otorgada se puede incrementar el rango de direcciones disponibles configuradas en el servidor DHCP para incrementar las cantidad de computadoras en la red.

Leonel F. Becchio

NAT-T

Si bien NAT nos ayuda a conservar el conjunto de direcciones disponibles remanentes en Internet, también introduce problemas relacionados con protocolos de comunicación end-to-end, como IPSec. Históricamente uno de los principales problemas relacionados con la implementación de comunicación L2TP/IPSec es que los equipos configurados para tal fin no pueden estar detrás de dispositivos NAT. Una nueva tecnología conocida como NAT-T (NAT Transversal) define cambios tanto en el proceso de negociación como así también en los diferentes métodos de envío de datos protegidos por IPSec.

Los dispositivos NAT-T compatibles automáticamente determinan durante el proceso de negociación IPSec:

Si ambos dispositivos (iniciador - generalmente una computadora cliente- y el dispositivo de recepción típicamente un servidor-) son dispositivos NAT-T compatibles.

Si se le realiza NAT a los paquetes enviados en el trayecto recorrido entre el iniciador y el receptor.

Si se cumplen AMBAS condiciones, los dispositivos automáticamente utilizan NAT-T para enviar tráfico protegido por IPSec a través de NAT.

Si alguno de los dispositivos no soporta NAT-T o bien no se realiza NAT entre los extremos de la sesión IPSec, se realiza una conexión IPSec estándar.

Nota: IPSec NAT-T está definido únicamente para tráfico ESP.

IPSec NAT-T es soportado por Windows Server 2003 (nativo), Windows 98-Windows ME-Windows NT instalando Microsoft L2TP/IPSec VPN Client y Windows 2000-Windows XP descargando el L2TP/IPSec NAT-T Update del sitio de Windows Update.




Cámara de las Empresas de Tecnología de la Información de Argentina. CESSI tiene más de 160 empresas socias y más de 300 a través de sus relaciones con otras instituciones, siendo así la entidad más representativa del sector. Estas empresas facturan el 70% del total de los negocios TICs en Argentina y emplean a más de 15.000 personas. CESSI defiende los intereses del sector y fomenta el uso de tecnologías de la información.

CEITI 04

cerró con buenas perspectivas para la industria



El sábado 26 de Junio 2004 concluyó el Congreso y

Jorge Cassino, presidente de CEITI, definió al encuentro de 3 días como "una fiesta de la industria" que contó con la participación de importantes figuras del empresariado y la destacada participación del vicepresidente de la Nación -en ejercicio del poder ejecutivo cuando se llevó a cabo el evento-, Daniel Scioli. El presidente del Senado de la Nación afirmó que la industria de software es estratégica para el país y se mostró muy esperanzado en su crecimiento. Entre las principales conclusiones de CEITI se destacan:

- Según TrendsConsulting/IDC Argentina: "El 79 por ciento de las 118 empresas que más tecnología consumen en el país (de hecho, la mitad de la que se vende entre todos los sectores) prefiere utilizar paquetes de desarrollo de software local" afirmó Raúl Bauer Director de la consultora.

- "En la Argentina nunca ha habido un plan de Ciencia y Técnica de largo plazo, podría decirse que ni siquiera de mediano plazo", señaló Tulio Abel del Bono, Secretario de Ciencia, Tecnología e Innovación Productiva de la Nación (SECyT), durante una disertación en el congreso. El funcionario nacional resumió durante su intervención las medidas que el organismo a su cargo ha tomado a lo largo de este año y las que se concretarán a lo largo de los meses siguientes en el área informático-tecnológica.

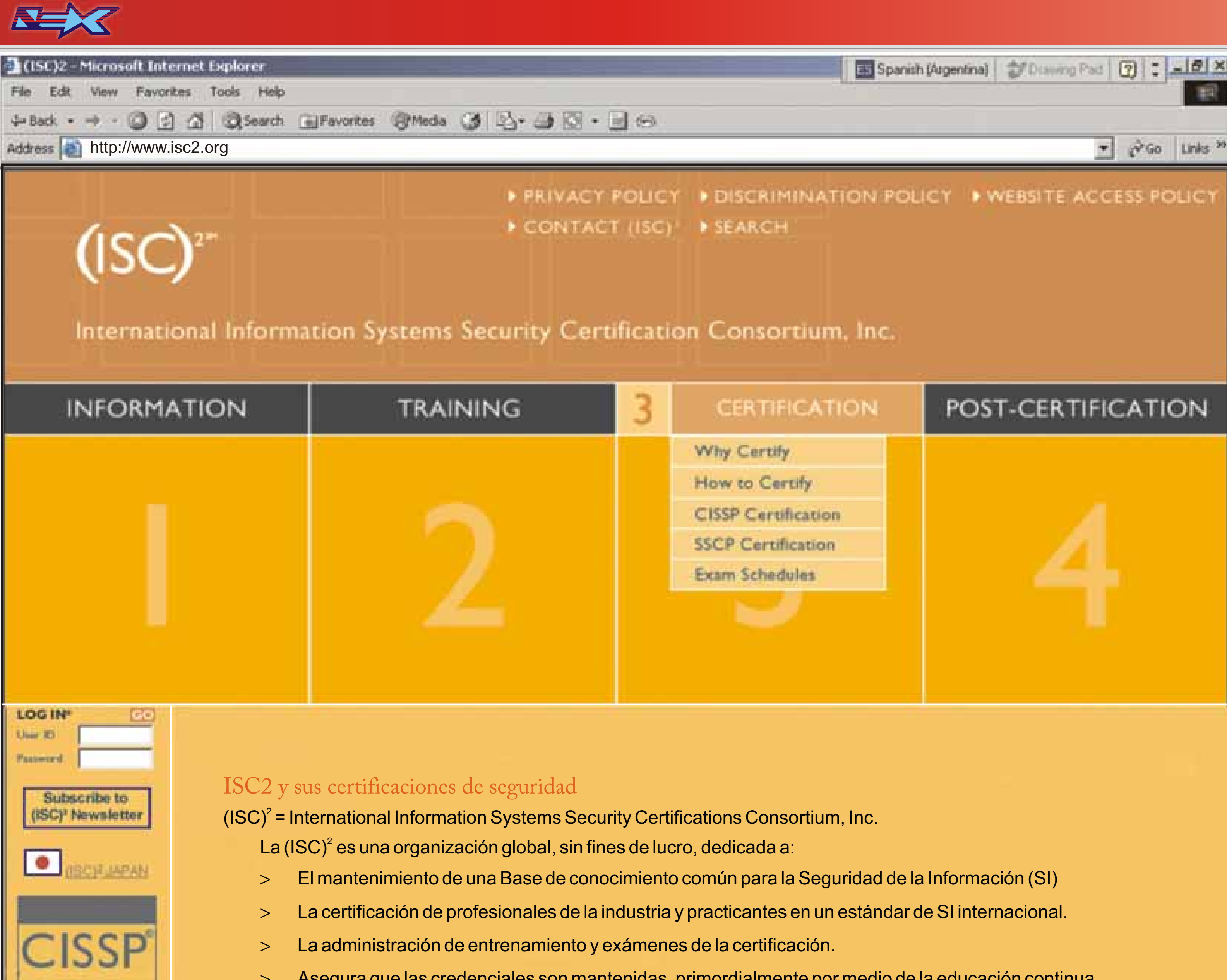
- Hace ya seis meses que los Foros de Competitividad industrial para nueve sectores a promocionar por el Gobierno Nacional están funcionando, y el del Software y Servicios Informáticos (SSI) es uno de ellos. Durante el Congreso y Exposición de las Tecnologías de la Información, CEITI 2004, funcionarios de la Secretaría de Industria explicaron en qué situación se encuentran las tareas del Foro y qué resultados podrán verse en los próximos meses. Durante el encuentro de CEITI 2004 se adelantaron diez de las principales acciones que el Plan contempla, y que será presentado en sociedad hacia fines del mes de julio.

- Sobre la relación comercial con China, Julio Werthein, Presidente de la Bolsa de Valores y también Presidente de la Cámara de la Producción, la Industria y el Comercio argentino-china, y Carlos Pallotti, Presidente de la Cámara de Empresas de Software y Servicios Informáticos (CESSI) firmaron un convenio de cooperación en el marco del Congreso y Exposición de la Industria de las Tecnologías de la Información (CEITI 2004) para potenciar la realización de negocios por parte de ambas cámaras en el país asiático.

DIGNO DE DESTACAR

CEITI nos mostró una Argentina en movimiento respecto del desarrollo del software. También nos mostró una entidad (CESSI) muy preocupada y activa, generando espacios de interacción y comunicación (CEITI 04).

Carlos Vaughn O`Connor



ISC2 y sus certificaciones de seguridad

(ISC)^2 = International Information Systems Security Certifications Consortium, Inc.

La (ISC)^2 es una organización global, sin fines de lucro, dedicada a:

> El mantenimiento de una Base de conocimiento común para la Seguridad de la Información (SI)

> La certificación de profesionales de la industria y practicantes en un estándar de SI internacional.

> La administración de entrenamiento y exámenes de la certificación.

> Asegura que las credenciales son mantenidas, primordialmente por medio de la educación continua.

Los gobiernos, corporaciones, centros de capacitación y organizaciones del mundo entero demandan una plataforma común para controlar la naturaleza dinámica de la seguridad de la información. (ISC)^2 ayuda a satisfacer estas necesidades.

Miles de profesionales en mas de 60 países han obtenido una certificación en una de las dos designaciones administradas por la (ISC)^2

> Certified Information Systems Security Professional [CISSP]

> System Security Certified Practitioner [SSCP]

Ambas credenciales indican que aquellos certificados han demostrado experiencia en el campo de seguridad de la información, aprobando un riguroso examen, subscribiéndose a un Código de Ética y manteniendo la certificación mediante educación continua.

¿Cómo certificarse?

Para convertirse en CISSP, un candidato debe en forma exitosa completar dos procesos:

1.Examen:

Los requerimientos para tomar el examen CISSP están completamente separados de los requerimientos necesarios para obtener la certificación.

Para tomar el examen CISSP, el candidato debe:

> Abonar el costo del examen.

> Demostrar que se posee una experiencia mínima de cuatro años de experiencia profesional en el campo de seguridad de la información o tres años mas un titulo universitario.

> Completar el Acuerdo del Candidato, atestiguando la experiencia profesional obtenida y adhiriéndose legalmente al Código de Ética CISSP.

> Responder exitosamente cuatro preguntas respecto a historia criminal y conceptos asociados.



2.Certificación:

Para serle otorgado el certificado, el candidato debe:

> Aprobar el examen CISSP con un puntaje de 700 puntos o superior.

> Enviar el Formulario de Consentimiento, adecuadamente completado y ejecutado.

> Si el candidato es elegido para una auditoria, deberá aprobar exitosamente la misma con respecto a sus afirmaciones de experiencia laborar.

Respaldo

Una vez que el candidato ha sido notificado de la aprobación del examen CISSP, el mismo deberá respaldar su aplicación con el consentimiento de otro CISSP, antes de que la certificación le sea otorgada. En el caso de que un CISSP no pueda ser ubicado, otro profesional calificado con conocimientos en Sistemas de Información o un superior del candidato puede ser utilizado para validad la experiencia profesional del candidato.

La certificación CISSP

La certificación CISSP fue diseñada para reconocer la maestría sobre un estándar internacional para la Seguridad de la Información y el conocimiento de la Base de conocimiento común. La certificación puede enriquecer la carrera profesional y brindar mayor credibilidad a la experiencia en SI

La estructura del examen

El examen de la certificación CISSP consiste en 250 preguntas de múltiple opción. Los candidatos tienen hasta 6 horas para completar el examen. Diez dominios de evaluación en seguridad de la información son cubiertos en el examen, todos pertenecientes a la Base de conocimiento común:

1. Metodología & Sistemas de Control de Acceso.
2. Desarrollo de Aplicaciones & Sistemas.
3. Planeamiento de la Continuidad del Negocio.
4. Criptografía.
5. Leyes, Investigación & Ética.
6. Seguridad de las Operaciones.
7. Seguridad Física.
8. Modelos & Arquitecturas de Seguridad.
9. Prácticas de administración de la seguridad.
10. Seguridad en las telecomunicaciones, redes & Internet.

La certificación CISSP en el mundo

Al día de la fecha existen aproximadamente 15.000 CISSP en todo el mundo. Su gran mayoría en los EEUU, donde se encuentra aproximadamente un 50%. Según un reciente estudio realizado por publicaciones especializadas, la certificación CISSP fue la más deseada, tanto por profesionales como empleadores durante el año 2002. El sueldo promedio anual de un profesional con la certificación CISSP en los EEUU se encuentra en el entorno de los U$S 85.000,00 anuales, siendo una de las certificaciones mejores pagas, y que generan mayores dividendos para los profesionales.



Microsoft



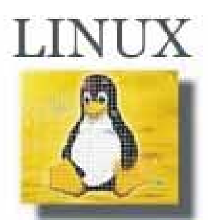
Security



WEB Design



LINUX



SUPLEMENTO GUÍA CURSOS Y CARRERAS - 1 AGOSTO 2004 A 31 JULIO 2005



Consultora en Capacitación Informática
Consultora en Seguridad Informática

www.cortech.com.ar

Garantía de Educación

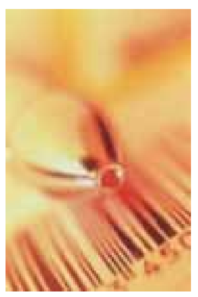


Un alumno, cuando "compra" un curso no busca otra cosa más que ADQUIRIR UN APRENDIZAJE, capacitarse, aprender, y crecer en el mundo de IT conociendo siempre las últimas tecnologías. La Garantía de aprendizaje COR, permite a TODOS los alumnos re-cursar cuantas veces sea necesario las Carreras o Cursos de COR TECH.

Aprovechá la posibilidad de volver a hacer tus cursos; ya sea si te quedaste con dudas, o faltaste alguna que otra clase, o simplemente porque deseas conocer el perfil de otro profesor o volver hacer el curso para conocer gente nueva.

En COR no comprás UN CURSO; comprás UN APRENDIZAJE (y queremos asegurarnos de dártelo).

Garantía de Precio



COR Technologies garantiza ofrecerte un precio 10 % más bajo para cualquier presupuesto de Educación o consultoría en Buenos Aires o en el Interior del País. Presentando el presupuesto de la competencia (ya sea por escrito o por e-mail; para un mínimo de 2 Alumnos ó mínimo de $1000) COR te brinda la Capacitación o la Solución buscada a un costo 10 % mas bajo (sólo multiplicá tu presupuesto por 0,90 y obtené el precio que te ofrece COR).

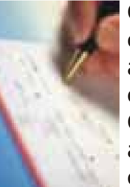
La Garantía de precio será respetada siempre y cuando el precio cobrado finalmente no sea menor al costo de realizar la Capacitación / Consultoría. COR Technologies se reserva el derecho de validación de los presupuestos propiamente presentados.

Garantía de Consultoría



Una característica de nuestras consultorías es que COR garantiza la completa conformidad de Cliente; o se reintegra el monto total de lo abonado para la misma. La Garantía de Consultoría permite al cliente estar confiado de que recibirá lo que desea; y que COR garantiza el resultado del problema mediante la Solución oportunamente propuesta.

COR Cheks



COR premia la Capacitación entregándole a todos nuestros alumnos la suma correspondiente de CORCheks. Cada CORChek es equivalente a un Peso; para ser utilizado en cualquiera de nuestros Cursos y Carreras. Los CORCheks no son transferibles; y no pueden utilizarse junto a otras promociones.

Microsoft Certified Systems Administrator (MCSA) Windows 2003

Microsoft CERTIFIED Technical Education Center

Microsoft CERTIFIED Partner for Learning Solutions

EXAMEN - Client	CURSO - Client
Examen 70–270: Installing, Configuring, and Administering Microsoft Windows XP Professional	**Curso 2285:** Installing, Configuring, and Administering Microsoft Windows XP Professional (Duración **16 hs**)
EXAMEN - Networking	**CURSO - Networking**
Examen 70–290: Managing and Maintaining a Microsoft Windows Server 2003 Environment	**Curso 2273:** Managing and Maintaining a Microsoft Windows Server 2003 Environment (Duración **40 hs**)
Examen 70–291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure	**Curso 2276:** Implementing a Microsoft Windows Server 2003 Network Infrastructure: Network Hosts (Duración **16 hs**)
	Curso 2277: Implementing, Managing, and Maintaining a MS Windows Server 2003 Network Infrastructure: Network Services (Duración **40 hs**)
EXAMEN - Elective	**CURSO - Elective**
Examen 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition	**Curso 2159:** Deploying and Managing Microsoft Internet Security and Acceleration Server 2000 (Duración **24 hs**)

Cursos: 5 (cinco) **MOC's incluidos: 5 (cinco)** **Duración Total: 136 hs**



Microsoft Certified Systems Administrator (MCSA Sec.) Security on Windows 2003 // Track Recomendado //

EXAMEN - Client	CURSO - Client
Examen 70–270: Installing, Configuring, and Administering Microsoft Windows XP Professional	**Curso 2285:** Installing, Configuring, and Administering Microsoft Windows XP Professional (Duración **16 hs**)
EXAMEN - Networking	**CURSO - Networking**
Examen 70–290: Managing and Maintaining a Microsoft Windows Server 2003 Environment	**Curso 2273:** Managing and Maintaining a Microsoft Windows Server 2003 Environment (Duración **40 hs**)
Examen 70–291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure	**Curso 2276:** Implementing a Microsoft Windows Server 2003 Network Infrastructure: Network Hosts (Duración **16 hs**)
	Curso 2277: Implementing, Managing, and Maintaining a MS Windows Server 2003 Network Infrastructure: Network Services (Duración **40 hs**)
EXAMEN - Elective	**CURSO - Elective**
Examen 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition	**Curso 2159:** Deploying and Managing Microsoft Internet Security and Acceleration Server 2000 (Duración **24 hs**)
Examen 70-299: Implementing and Administering Security in a Microsoft Windows Server 2003 Network	**Curso 2823:** Implementing and Administering Security in a Microsoft Windows Server 2003 Network (Duración **40 hs**)

Cursos: 6 (seis) **MOC's incluidos: 6 (seis)** **Duración Total: 176 hs**

Fechas Inicio Calendario

MCSA y MCSA Security

INICIO	DIAS	HORARIO
03-08-04	M-J	9.00 a 13.00
13-08-04	L-M-V	18.30 a 22.30
14-08-04	M-J	18.30 a 22.30
03-09-04	L-M-V	9.00 a 13.00
10-09-04	M-J	9.00 a 13.00
07-09-04	L-M-V	18.30 a 22.30
05-10-04	M-J	18.30 a 22.30
12-10-04	M-J	9.00 a 13.00
13-10-04	L-M-V	18.30 a 22.30
02-11-04	M-J	9.00 a 13.00
10-11-04	L-M-V	18.30 a 22.30
16-11-04	L-M-V	9.00 a 13.00
04-01-05	M-J	18.30 a 22.30
14-01-05	L-M-V	18.30 a 22.30
19-01-05	L-M-V	9.00 a 13.00
08-02-05	M-J	9.00 a 13.00
11-02-05	L-M-V	9.00 a 13.00
18-02-05	L-M-V	18.30 a 22.30
15-03-05	M-J	9.00 a 13.00
18-03-05	L-M-V	18.30 a 22.30
10-03-05	M-J	18.30 a 22.30
19-04-05	M-J	18.30 a 22.30
15-04-05	M-J	9.00 a 13.00
13-04-05	L-M-V	9.00 a 13.00
04-05-05	M-J	18.30 a 22.30
10-05-05	M-J	9.00 a 13.00
18-05-05	L-M-V	18.30 a 22.30
07-06-05	M-J	9.00 a 13.00
15-06-05	L-M-V	18.30 a 22.30
17-06-05	L-M-V	9.00 a 13.00
05-07-05	M-J	18.30 a 22.30
13-07-05	L-M-V	18.30 a 22.30
15-07-05	L-M-V	9.00 a 13.00

Para más información sobre la carrera MCSA Windows 2003 visitá www.cortech.com.ar/ms/mcsa.htm ó www.microsoft.com/learning/mcp/mcsa/default.asp

Certificaciones Internacionales

¿Dónde se pueden rendir los exámenes para certificarme como MCSA y/o MCSE?

Podés hacer los exámenes en cualquier centro CTEC (Certified Training Education Center) de tu localidad que provea exámenes VUE: Virtual Universities Enterprise (ver www.vue.com)

Deberás entonces reservar tu turno de examen y abonar el costo correspondiente de 125.00 U$S en U.S.A. por examen; y 80.00 U$S en Argentina (tarifas adicionales o descuentos pueden aplicarse en otras regiones).

Todos los Tracks MCSA

¿Cuáles son los Exámenes que debo tomar para recibirme de MCSA?

Existen muchísimas combinaciones de Exámenes para recibirse de MCSA: Microsoft Certified Systems Administrator. Cada una con diferentes especializaciones y electivos para tomar.

MCSA

http://www.cortech.com.ar/gen/mcsawin2003.pdf
http://www.cortech.com.ar/gen/MCSASec2000-2003.pdf
http://www.cortech.com.ar/gen/MCSAMes2000-2003.pdf

Microsoft Certified Systems Engineer (MCSE) Windows 2003

Microsoft CERTIFIED Technical Education Center

Microsoft CERTIFIED Partner for Learning Solutions

EXAMEN - Client	CURSO - Client
Examen 70–270: Installing, Configuring, and Administering Microsoft Windows XP Professional	**Curso 2285:** Installing, Configuring, and Administering Microsoft Windows XP Professional (Duración **16 hs**)
EXAMEN - Networking	**CURSO - Networking**
Examen 70–290: Managing and Maintaining a Microsoft Windows Server 2003 Environment	**Curso 2273:** Managing and Maintaining a Microsoft Windows Server 2003 Environment (Duración **40 hs**)
Examen 70–291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure	**Curso 2276:** Implementing a Microsoft Windows Server 2003 Network Infrastructure: Network Hosts (Duración **16 hs**)
	Curso 2277: Implementing, Managing, and Maintaining a MS Windows Server 2003 Network Infrastructure: Network Services (Duración **40 hs**)
Examen 70-293: Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure	**Curso 2278:** Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure (Duración **40 hs**)
Examen 70-294: Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure	**Curso 2279:** Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure (Duración **40 hs**)
EXAMEN - Design	**CURSO - Design**
Examen 70-298: Designing Security for a Microsoft Windows Server 2003 Network	**Curso 2830:** Designing Security for Microsoft Networks (Duración **24 hs**)
EXAMEN - Elective	**CURSO - Elective**
Examen 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition	**Curso 2159:** Deploying and Managing Microsoft Internet Security and Acceleration Server 2000 (Duración **24 hs**)
# Cursos: 8 (ocho) **MOC's incluidos: 8 (ocho)**	**Duración Total: 240 hs**

Microsoft Certified Systems Engineer (MCSE Sec.) Security on Windows 2003 (Carrera MCSE + Examen 70-299)

Examen 70-299: Implementing and Administering Security in a Microsoft Windows Server 2003 Network	**Curso 2823:** Implementing and Administering Security in a Microsoft Windows Server 2003 Network (Duración **40 hs**)
# Cursos: 9 (nueve) **MOC's incluidos: 9 (nueve)**	**Duración Total: 280 hs**

Microsoft Certified Systems Engineer // Track Recomendado // Security + 2282 on Win. 2003 (Carrera MCSE Security + Examen 70-297)

Examen 70-297: Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure	**Curso 2282:** Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure (Duración **40 hs**)
# Cursos: 10 (diez) **MOC's incluidos: 10 (diez)**	**Duración Total: 320 hs**



Fechas Inicio Calendario

MCSE, MCSE Security y MCSE Sec + 2282

INICIO	DIAS	HORARIO
10-08-04	M-J	9.00 a 13.00
20-08-04	L-M-V	18.30 a 22.30
21-08-04	M-J	18.30 a 22.30
10-09-04	L-M-V	9.00 a 13.00
17-09-04	M-J	9.00 a 13.00
14-09-04	L-M-V	18.30 a 22.30
12-10-04	M-J	18.30 a 22.30
19-10-04	M-J	9.00 a 13.00
20-10-04	L-M-V	18.30 a 22.30
09-11-04	M-J	9.00 a 13.00
17-11-04	L-M-V	18.30 a 22.30
23-11-04	L-M-V	9.00 a 13.00
11-01-05	M-J	18.30 a 22.30
21-01-05	L-M-V	18.30 a 22.30
26-01-05	L-M-V	9.00 a 13.00
15-02-05	M-J	9.00 a 13.00
18-02-05	L-M-V	9.00 a 13.00
25-02-05	L-M-V	18.30 a 22.30
22-03-05	M-J	9.00 a 13.00
25-03-05	L-M-V	18.30 a 22.30
17-03-05	M-J	18.30 a 22.30
26-04-05	M-J	18.30 a 22.30
22-04-05	M-J	9.00 a 13.00
20-04-05	L-M-V	9.00 a 13.00
11-05-05	M-J	18.30 a 22.30
17-05-05	M-J	9.00 a 13.00
25-05-05	L-M-V	18.30 a 22.30
14-06-05	M-J	9.00 a 13.00
22-06-05	L-M-V	18.30 a 22.30
24-06-05	L-M-V	9.00 a 13.00
12-07-05	M-J	18.30 a 22.30
20-07-05	L-M-V	18.30 a 22.30
22-07-05	L-M-V	9.00 a 13.00

Para más información sobre la carrera MCSE Windows 2003 visitá www.cortech.com.ar/ms/mcse.htm ó www.microsoft.com/learning/mcp/mcse/default.asp

Todos los Tracks MCSE

¿Cuáles son los Exámenes que debo tomar para recibirme de MCSE?

Existen muchísimas combinaciones de Exámenes para recibirse de MCSE: Microsoft Certified Systems Engineer. Cada una con diferentes especializaciones y electivos para tomar.

MCSE

http://www.cortech.com.ar/gen/mcsewin2003.pdf
http://www.cortech.com.ar/gen/MCSESec2000-2003.pdf
http://www.cortech.com.ar/gen/MCSEMes2000-2003.pdf

Logos MCP

¿Cuáles son los logos que podré utilizar cuándo me reciba de MCP, MCSA, MCSE, MCDBA, MCAD ó MCSD?¿Existe alguna diferencia entre los logos con especializaciones en Security, Messaging, etc..?

Al finalizar de haber rendido todos los Exámenes de cada Carrera Microsoft, podrás utilizar el logo correspondiente. Todos las Carreras (como así tambien las especializaciones) poseen un logo diferente.

Podés encontrar todos los logos Microsoft correspondientes en http://www.microsoft.com/learning/mcpexams/faq/logo.asp



www.cortech.com.ar

Microsoft Certified Application Developer (MCAD) Visual Basic .NET

Microsoft CERTIFIED Technical Education Center

Microsoft CERTIFIED Partner for Learning Solutions

EXAMEN - Módulo I	CURSO - Módulo I
Examen 70-305: Developing and Implementing Web Applications with Microsoft® Visual Basic® .NET and Microsoft® Visual Studio® .NET	**Curso 2559:** Introduction to Visual Basic .NET Programming with Microsoft .NET (Duración **20 hs**)
	Curso 2310: Developing Microsoft ASP.NET Web Applications Using Visual Studio .NET (Duración **40 hs**)
EXAMEN - Módulo II	**CURSO - Módulo II**
Examen 70-310: Developing XML Web Services and Server Components with Microsoft® Visual Basic® .NET and the Microsoft® .NET Framework	**Curso 2415:** Programming with the Microsoft® .NET Framework (Microsoft V. Basic® .NET) (Duración **40 hs**)
	Curso 2524: Developing XML Web Services Using Microsoft® ASP.NET (Duración **20 hs**)
	Curso 2557: Building COM+ Applications Using Microsoft® .NET Enterprise Services (Duración **20 hs**)
EXAMEN - Módulo III	**CURSO - Módulo III**
Examen 70-229: Designing and Impl. Databases with MS SQL Server 2000™ Enterprise Edition	**Curso 2073:** Programming a Microsoft SQL Server 2000 Database (Duración **40 hs**)
# Cursos: 6 (seis) **MOC's incluidos: 6 (seis)**	**Duración Total: 180 hs**

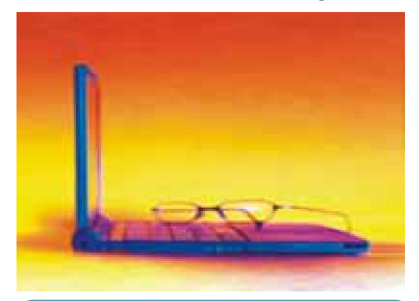
Microsoft Certified Solution Developer (MCSD) Visual Basic .NET (Carrera MCAD + Examen 70-300 + Examen 70-306)

EXAMEN - Módulo IV	CURSO - Módulo IV
Examen 70-300: Analyzing Requirements & Defining .NET Solution Architectures	**Curso 2710 :** Analyzing Requirements and Defining .NET Solution Architecture (Duración **40 hs**)
EXAMEN - Módulo V	**CURSO - Módulo V**
Examen 70-306: Developing & Impementing Windows-based Applications with Microsoft Visual Basic .NET & MS Visual Studio .NET	**Curso 2565:** Developing Microsoft .NET Applications for Windows (Visual Basic .NET) (Duración **20 hs**)
# Cursos: 8 (ocho) **MOC's incluidos: 8 (ocho)**	**Duración Total: 240 hs**

Microsoft Certified Application Developer (MCAD) C#™ .NET

// Track Recomendado //

EXAMEN - Módulo I	CURSO - Módulo I
Examen 70-315: Developing and Implementing Web Applications with Microsoft Visual C#™ .NET and Microsoft Visual Studio .NET	**Curso 2609:** Introduction to C# Programming with Microsoft .NET (Duración **20 hs**)
	Curso 2310: Developing Microsoft ASP.NET Web Applications Using Visual Studio .NET (Duración **40 hs**)
EXAMEN - Módulo II	**CURSO - Módulo II**
Examen 70-320: Developing XML Web Services and Server Components with Microsoft Visual C# and the Microsoft .NET Framework	**Curso 2349:** Programming with the Microsoft .NET Framework (Microsoft Visual C# .NET).(Duración **40 hs**)
	Curso 2524: Developing XML Web Services Using Microsoft® ASP.NET (Duración **20 hs**)
	Curso 2557: Building COM+ Applications Using Microsoft® .NET Enterprise Services (Duración **20 hs**)
EXAMEN - Módulo III	**CURSO - Módulo III**
Examen 70-229: Designing and Impl. Databases with MS SQL Server 2000™ Enterprise Edition	**Curso 2073:** Programming a Microsoft SQL Server 2000 Database (Duración **40 hs**)
# Cursos: 6 (seis) **MOC's incluidos: 6 (seis)**	**Duración Total: 180 hs**



SQL Server

Las dos Certificaciones de SQL más importantes son: **Examen 70-228** (Installing, Configuring, and Administering Microsoft SQL Server 2000 Enterprise Edition) y **Examen 70-229** (Designing and Implementing Databases with Microsoft SQL Server 2000 Enterprise Edition).

Estos Exámenes podrán prepararse con los Cursos Oficiales **2072** (Administering a MS-SQL Server 2000 Database) y **2073** (Programming a MS-SQL Server 2000 Database) respectivamente.

Fechas Inicio Calendario

MCAD V. Basic, MCSD y MCAD C#

INICIO	DIAS	HORARIO
03-08-04	M-J	9.00 a 13.00
13-08-04	L-M-V	18.30 a 22.30
14-08-04	M-J	18.30 a 22.30
03-09-04	L-M-V	9.00 a 13.00
10-09-04	M-J	9.00 a 13.00
07-09-04	L-M-V	18.30 a 22.30
05-10-04	M-J	18.30 a 22.30
12-10-04	M-J	9.00 a 13.00
13-10-04	L-M-V	18.30 a 22.30
02-11-04	M-J	9.00 a 13.00
10-11-04	L-M-V	18.30 a 22.30
16-11-04	L-M-V	9.00 a 13.00
04-01-05	M-J	18.30 a 22.30
14-01-05	L-M-V	18.30 a 22.30
19-01-05	L-M-V	9.00 a 13.00
08-02-05	M-J	9.00 a 13.00
11-02-05	L-M-V	9.00 a 13.00
18-02-05	L-M-V	18.30 a 22.30
15-03-05	M-J	9.00 a 13.00
18-03-05	L-M-V	18.30 a 22.30
10-03-05	M-J	18.30 a 22.30
19-04-05	M-J	18.30 a 22.30
15-04-05	M-J	9.00 a 13.00
13-04-05	L-M-V	9.00 a 13.00
04-05-05	M-J	18.30 a 22.30
10-05-05	M-J	9.00 a 13.00
18-05-05	L-M-V	18.30 a 22.30
07-06-05	M-J	9.00 a 13.00
15-06-05	L-M-V	18.30 a 22.30
17-06-05	L-M-V	9.00 a 13.00
05-07-05	M-J	18.30 a 22.30
13-07-05	L-M-V	18.30 a 22.30
15-07-05	L-M-V	9.00 a 13.00

Para más información sobre la carrera MCAD .NET, MCSD y MCAD C# visitá www.cortech.com.ar/ms/ms4.htm ó www.microsoft.com/learning/mcp/mcad/

Links Microsoft

¿Existe algún link en donde se puedan ver todos los Exámenes actuales de Microsoft y todos sus Cursos Oficiales asociados?

Para ver todos los Exámenes Microsoft vigentes que existen visitá **www.microsoft.com/learning/mcpexams/prepare/findexam.asp** Allí los podrás visualizar por Carreras o por número de Examen.

Y para ver todos los Cursos Oficiales vigentes visitá **www.microsoft.com/traincert/training/find/findcourse.asp** Allí podrás visualizarlos por Producto o por número de Curso.

Carrera MCDBA

¿Cuáles son los exámenes que debo tomar para realizar la Carrera MCDBA?

Para ver el listado completo de todas las opciones que existen para convertirte en Microsoft Certified Data Base Administrator (MCDBA) te recomendamos visitar la siguiente página WEB: http://www.microsoft.com/learning/mcp/mcdba/default.asp.

El Track recomendado para convertirte en MCDBA es realizar la Carrera MCSE de 240 hs de Duración (7 Exámenes) + los Exámenes de SQL Server 70-228 (Administering) y 70-229 (Programming)

Fechas Inicio Calendario
WEB Design Completa y Expert

INICIO	DIAS	HORARIO
06-08-04	L-M-V	9.30 a 12.30
12-08-04	M-J	18.30 a 21.30
17-08-04	M-J	14.00 a 17.00
04-09-04	S	10.00 a 13.00
08-09-04	L-M-V	18.30 a 21.30
16-09-04	M-J	9.30 a 12.30
01-10-04	L-M-V	9.30 a 12.30
07-10-04	M-J	18.30 a 21.30
13-10-04	L-M-V	14.00 a 17.00
06-11-04	S	10.00 a 13.00
10-11-04	L-M-V	18.30 a 21.30
18-11-04	M-J	9.30 a 12.30
07-01-05	L-M-V	9.30 a 12.30
13-01-05	M-J	18.30 a 21.30
18-01-05	M-J	14.00 a 17.00
05-02-05	S	10.00 a 13.00
11-02-05	L-M-V	18.30 a 21.30
17-02-05	M-J	9.30 a 12.30
04-03-05	L-M-V	9.30 a 12.30
17-03-05	M-J	18.30 a 21.30
18-03-05	L-M-V	14.00 a 17.00
09-04-04	S	10.00 a 13.00
08-04-05	L-M-V	18.30 a 21.30
21-04-05	M-J	9.30 a 12.30
13-05-04	L-M-V	9.30 a 12.30
12-05-05	M-J	18.30 a 21.30
19-05-05	M-J	14.00 a 17.00
11-06-05	S	10.00 a 13.00
15-06-05	L-M-V	18.30 a 21.30
16-06-05	M-J	9.30 a 12.30
06-07-05	L-M-V	9.30 a 12.30
14-07-05	M-J	18.30 a 21.30
20-07-05	L-M-V	14.00 a 17.00

Carrera WEB Design Completa
WEB1 + WEB2 + WEB3

EXAMEN - WEB Design	CURSO - WEB Design
Examen Dreamweaver MX 2004 Designer	**Módulo WEB1:** Curso de Front Page XP y Macromedia Dreamweaver MX 04 (Duración **18 hs**)
Exámenes Flash MX 2004 Designer y Developer	**Módulo WEB2:** Curso de Macromedia Flash MX 04 y Macromedia Fireworks MX 04 (Duración **21 hs**)
Exámenes Dreamweaver MX 2004 Designer y Developer	**Módulo WEB3:** Curso de Edición HTML e Introd. a Programación ASP (Duración **21 hs**)
# Cursos: 3 (tres) **WOG's incluidos: 1 (uno)**	**Duración Total: 60 hs**

Carrera WEB Design Expert
WEB1 + WEB2 + WEB3 + WEB4 + WEB5 // Track Recomendado //

EXAMEN - WEB Design	CURSO - WEB Developer
Examen Dreamweaver MX 2004 Developer	**Módulo WEB4:** Curso Programación ASP Avanzado (Duración **21 hs**)
-- --	**Módulo WEB5:** Curso Programación PHP Avanzado (Duración **21 hs**)
# Cursos: 5 (cinco) **WOG's incluidos: 2 (dos)**	**Duración Total: 102 hs**

Para más información sobre la carrera WEB Design Completa y WEB Design Expert visitá www.cortech.com.ar/web/web1.htm



Carrera COR Security // Track Recomendado //
SEC1 + SEC2 + Especialización (a elección)

EXAMEN - CISSP	CURSO - Security
CISSP: Certified Information Systems Security Professional	**Clínica SEC1:** Seguridad y sus fundamentos (Duración **20 hs**) **Clínica SEC2:** Seguridad Avanzada (Duración **20 hs**)
Especialización LINUX	**Especialización Microsoft**
Módulo LX5: Seguridad y contra-seguridad en Redes (Duración **12hs**) + **Workshop LX6:** Workshops Servidor de Firewall y Squid (Comparación con ISA Server) (Duración **12 hs**) + **Workshop LX8:** Workshops Implementando VPNs bajo Linux (Duración **12 hs**)	**Curso 2159:** Deploying and Managing Microsoft Internet Security and Acceleration Server 2000 (Duración **24 hs**) + **Curso 40 hs Seguridad Electivo** de la Currícula Oficial Microsoft + **Curso 2823:** Implementing and Administering Security in a Microsoft Windows Server 2003 Network (Duración **40 hs**)
Incluye Material **# Cursos: 5 (cinco)** **Duración Total: 76 hs**	**Incluye Material** **# Cursos: 5 (cinco)** **Duración Total: 144 hs**

Para más información sobre la carrera COR Security y sus Especializaciones visitá www.secure105.com.ar

Fechas Inicio Calendario
Carrera COR Security + Especializaciones

INICIO	DIAS	HORARIO
17-08-04	M-J	9.00 a 13.00
27-08-04	L-M-V	18.30 a 22.30
28-08-04	M-J	18.30 a 22.30
17-09-04	L-M-V	9.00 a 13.00
24-09-04	M-J	9.00 a 13.00
21-09-04	L-M-V	18.30 a 22.30
19-10-04	M-J	18.30 a 22.30
26-10-04	M-J	9.00 a 13.00
27-10-04	L-M-V	18.30 a 22.30
16-11-04	M-J	9.00 a 13.00
24-11-04	L-M-V	18.30 a 22.30
30-11-04	L-M-V	9.00 a 13.00
18-01-05	M-J	18.30 a 22.30
28-01-05	L-M-V	18.30 a 22.30
02-02-05	L-M-V	9.00 a 13.00
22-02-05	M-J	9.00 a 13.00
25-02-05	L-M-V	9.00 a 13.00
04-03-05	L-M-V	18.30 a 22.30
29-03-05	M-J	9.00 a 13.00
01-04-05	L-M-V	18.30 a 22.30
24-03-05	M-J	18.30 a 22.30
03-05-05	M-J	18.30 a 22.30
29-04-05	M-J	9.00 a 13.00
27-04-05	L-M-V	9.00 a 13.00
18-05-05	M-J	18.30 a 22.30
24-05-05	M-J	9.00 a 13.00
01-06-05	L-M-V	18.30 a 22.30
21-06-05	M-J	9.00 a 13.00
29-06-05	L-M-V	18.30 a 22.30
01-07-05	L-M-V	9.00 a 13.00
19-07-05	M-J	18.30 a 22.30
27-07-05	L-M-V	18.30 a 22.30
29-07-05	L-M-V	9.00 a 13.00

Cursos Intensivos y Personalizados

¿Cómo puedo hacer para que yo o la gente de mi Empresa pueda cursar cualquiera de los Cursos y Carreras Microsoft, Security, WEB Design o Linux de manera Personalizada / Intensiva?

Te recomendamos averiguar por costos y metodologías de cursada de todos nuestros Cursos y Carreras para realizarlos de forma intensiva y personalizada ya sea en las Oficinas de COR TECH o in Company (Capital o Interior del País).
Enviando solamente un email a intensive@cortech.com.ar o llamando al (54)11-4312-7694.

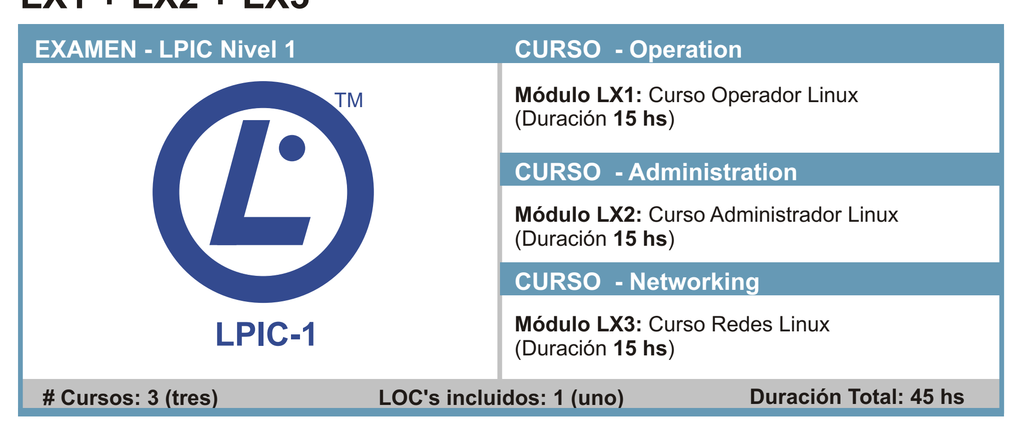
Certificaciones Macromedia

¿Dónde se pueden rendir los exámenes para certificarme como Macromedia Dreamweaver MX 2004 Designer, Developer y Flash MX 2004 Designer, Developer?

Podés hacer los exámenes en cualquier centro de tu localidad que provea exámenes VUE: Virtual Universities Enterprise (ver www.vue.com). Deberás entonces reservar tu turno de examen y abonar el costo correspondiente de 150.00 U$S para cada Examen MX 2004.

Más información respecto de las Certificaciones Macromedia MX 2004 podrás encontrarla en **www.macromedia.com**

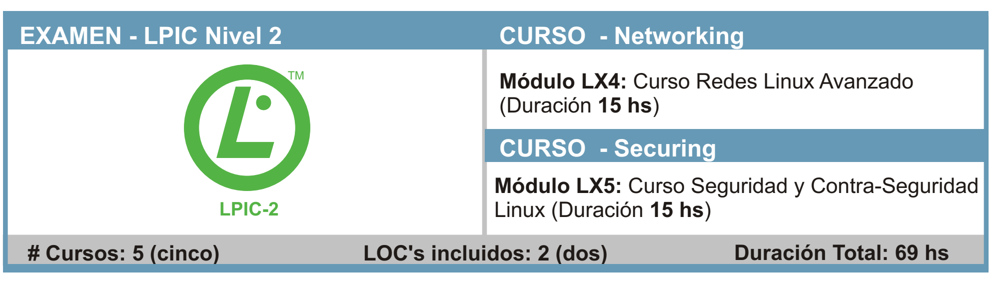
Carrera Linux Completa
LX1 + LX2 + LX3



EXAMEN - LPIC Nivel 1	CURSO - Operation
LPIC-1	**Módulo LX1:** Curso Operador Linux (Duración **15 hs**)
	CURSO - Administration
	Módulo LX2: Curso Administrador Linux (Duración **15 hs**)
	CURSO - Networking
	Módulo LX3: Curso Redes Linux (Duración **15 hs**)

Cursos: 3 (tres) **LOC's incluidos: 1 (uno)** **Duración Total: 45 hs**

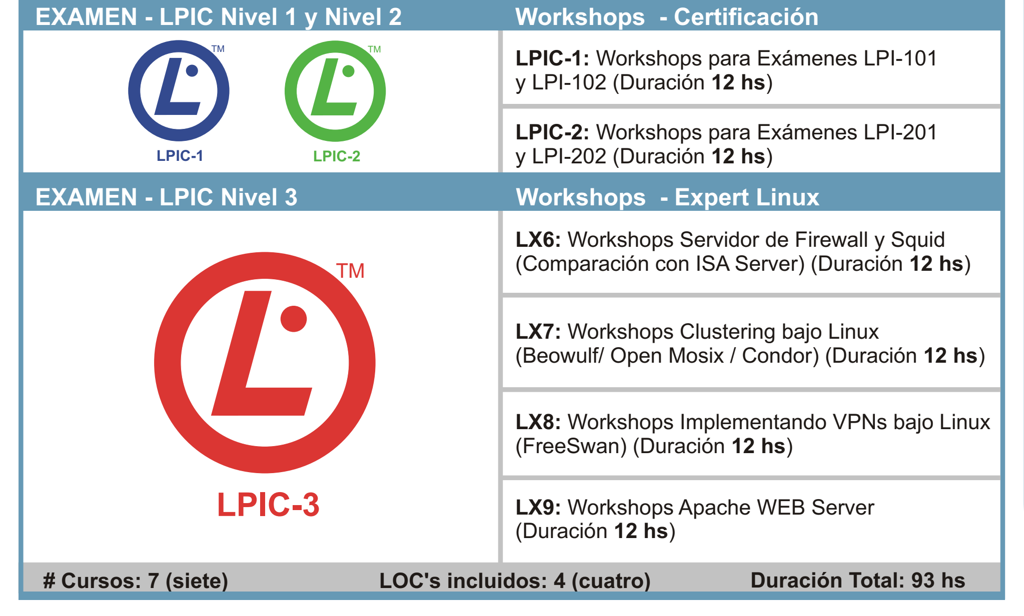
Carrera Linux Avanzada
LX1 + LX2 + LX3 + LX4 + LX5



EXAMEN - LPIC Nivel 2	CURSO - Networking
LPIC-2	**Módulo LX4:** Curso Redes Linux Avanzado (Duración **15 hs**)
	CURSO - Securing
	Módulo LX5: Curso Seguridad y Contra-Seguridad Linux (Duración **15 hs**)

Cursos: 5 (cinco) **LOC's incluidos: 2 (dos)** **Duración Total: 69 hs**

Carrera Linux Expert // Track Recomendado //
LX1 + LX2 + LX3 + LX4 + LX5 + 2 Workshops LX (a elección)



EXAMEN - LPIC Nivel 1 y Nivel 2	Workshops - Certificación
LPIC-1 LPIC-2	**LPIC-1:** Workshops para Exámenes LPI-101 y LPI-102 (Duración **12 hs**)
	LPIC-2: Workshops para Exámenes LPI-201 y LPI-202 (Duración **12 hs**)
EXAMEN - LPIC Nivel 3	**Workshops - Expert Linux**
LPIC-3	**LX6:** Workshops Servidor de Firewall y Squid (Comparación con ISA Server) (Duración **12 hs**)
	LX7: Workshops Clustering bajo Linux (Beowulf/ Open Mosix / Condor) (Duración **12 hs**)
	LX8: Workshops Implementando VPNs bajo Linux (FreeSwan) (Duración **12 hs**)
	LX9: Workshops Apache WEB Server (Duración **12 hs**)

Cursos: 7 (siete) **LOC's incluidos: 4 (cuatro)** **Duración Total: 93 hs**

debian





Fechas Inicio Calendario
Carrera Linux Complete, Advanced y Expert

INICIO	DIAS	HORARIO
11-08-04	L-M-V	9.30 a 12.30
14-08-04	S	10.00 a 13.00
18-08-04	M-J	18.30 a 21.30
03-09-04	L-M-V	18.30 a 21.30
09-09-04	M-J	9.30 a 12.30
14-09-04	M-J	14.00 a 17.00
06-10-04	L-M-V	9.30 a 12.30
09-10-04	S	10.00 a 13.00
14-10-04	M-J	18.30 a 21.30
05-11-04	L-M-V	18.30 a 21.30
11-11-04	M-J	9.30 a 12.30
12-11-04	L-M-V	14.00 a 17.00
05-01-05	L-M-V	9.30 a 12.30
08-01-05	S	10.00 a 13.00
13-01-05	M-J	18.30 a 21.30
04-02-05	L-M-V	18.30 a 21.30
10-02-05	M-J	9.30 a 12.30
15-02-05	M-J	14.00 a 17.00
04-03-05	L-M-V	9.30 a 12.30
12-03-05	S	10.00 a 13.00
17-03-05	M-J	18.30 a 21.30
06-04-05	L-M-V	18.30 a 21.30
14-04-05	M-J	9.30 a 12.30
08-04-05	L-M-V	14.00 a 17.00
04-05-05	L-M-V	9.30 a 12.30
07-05-05	S	10.00 a 13.00
12-05-05	M-J	18.30 a 21.30
08-06-05	L-M-V	9.30 a 12.30
09-06-05	M-J	18.30 a 21.30
14-06-05	M-J	14.00 a 17.00
01-07-05	L-M-V	18.30 a 21.30
14-07-05	M-J	9.30 a 12.30
16-07-05	S	10.00 a 13.00

Para más información sobre la carrera Linux Completa, Avanzada y Expert visitá www.cortech.com.ar/lxc/lxc1.htm

Costos de las Carreras y Cursos

¿Dónde se puede averiguar el costo de los Cursos y Carreras Microsoft, Security, WEB Design y/o Linux?

Podés averiguar los costos de los Cursos y Carreras acercándote personalmente a COR Technologies SRL: Av. Córdoba 657 Piso 12, telefónicamente llamando al (54)11-4312-7694, vía correo electrónico a masinfo@cortech.com.ar, o en http://www.cortech.com.ar

http://www.cortech.com.ar/gen/Cursos y Fechas COR.pdf

Certificaciones LPI

¿Dónde se pueden rendir los exámenes para certificarme en LPIC 101, 102, 201 ó 202?

Podés hacer los exámenes en cualquier centro de tu localidad que provea exámenes VUE: Virtual Universities Enterprise (ver www.vue.com)

Deberás entonces reservar tu turno de examen y abonar el costo correspondiente de 150.00 U$S para cada Examen.

Más información respecto de las Certificaciones LPI podrás encontrarla en **www.lpi.org**